Territory of Guam

HEALTH INFORMATION EXCHANGE COOPERATIVE AGREEMENT PROGRAM

GUAM'S 2012 STRATEGIC AND OPERATIONAL PLAN UPDATE

Submitted to the Office of the National Coordinator for Health Information Technology by the Guam eHealth Collaborative

January 18, 2013

Table of Contents

1.0 BACKGROUND

BACKGROUND

Guam is located approximately 3,300 miles West of Hawaii, 1,500 miles east of the Philippines and 1,550 miles south of Japan. The island is the Western-most territory of the United States and is one of the leading tourist destinations in the Western Pacific. The total population of Guam in 2008 was 192,805 persons, as released by the U.S. Bureau of the Census in June 2008.

Guam offers some significant health care advantages to Americans living in Asia. Guam's health care system includes two major hospitals (one civilian and one military), a widespread clinic network, a broad selection of general and specializing physicians, and medical evacuation operations to Hawaii, the U.S. mainland and the Philippines. The island's two hospital facilities are the Naval Regional Medical Center and Guam Memorial Hospital. While the Naval hospital provides services to veterans, active-duty personnel and military dependents, Guam Memorial Hospital provides the only hospital care for the remainder of the general public. The Guam Memorial Hospital is the only publicly owned facility operated as part of the government of Guam.

Guam has ten specialty and emergency care clinics and about 30 pharmacies for prescription drug needs. Specialized healthcare facilities include Guam Radiology Consultants, 2 renal care facilities, Guam's first privately owned and operated birthing center, a surgical center for outpatient surgical procedures, and the Heart & Vascular Institute of Guam.

The medical board of physicians on Guam has set standards for practitioners which are similar to those in California. All doctors must be U.S. trained and board eligible to practice on Guam.

There are a total of about 150 physicians licensed on Guam with 87 of the most highly consumer-rated clinicians in Guam comprising of:
- 4 professional staff from the Guam Department of Public Health and Social Services
- 16 Public Health Nurses from DPHSS
- 12 family practice clinicians
- 16 physicians from the Guam Medical Society
- 31 labor and delivery clinical staff from Guam Memorial Hospital
- 6 staff from Sagua Managua birthing center
- 2 pediatricians from the Naval Hospital

The organization of healthcare is similar to that of the mainland US in terms of medical licensure requirements, types of healthcare providers, and a public-private healthcare system, which focuses on acute care rather than preventive services. Several public and private insurance companies serve the population of Guam. Public health insurance includes federal

Medicare and Medicaid programs, as well as a locally funded insurance program called Medically Indigent Program (MIP).

- Medicare enrolls about 2,000 Guam Seniors.
- Medicaid enrolls about 8,000 people.

There is an overall lack of government funding and resources, particularly with respect to medical specialists. Most patients who require the immediate attention of specialists must go off island to Hawaii, resulting in gaps in communication and coordination among providers caring for those patients.

A reduction in human and financial resources has severely impacted the health system. An early retirement program, instituted at the end of 1999, led many experienced health workers to retire. While the vacated positions have continued to be funded, there is not a large enough resource pool to fill all of them. Tightening government budgets have left some less critical positions vacant, and these vacancies have reduced the overall amount of services available to the uninsured and underinsured population. The vacancies have also affected progress in strengthening other health service priority areas, such as disposal of hazardous and toxic materials, environmental protection, vector control, and drug and alcohol abuse services.

All public health services depend on having a basic infrastructure, especially in terms of personnel. Unfortunately, Guam is experiencing health workforce shortages due to the early retirement of its most experienced professionals. Human resources for health are still lacking in critical areas and must be developed locally to the greatest extent possible.

The Division of Environmental Health of the Department of Public Health and Social Services (DPHSS) is also understaffed. Over half the Division's staff has fewer than five years' experience, and staff generally lacks specialized training.

All health care products, from toothbrushes to prescription medications, are regulated and monitored by the Drug and Medical Device Program. Because of Guam's geographical location and the ethnic diversity of its people, various drugs and medical devices of foreign origin are imported, distributed and marketed. These include many poorly labeled, misbranded and adulterated drugs, as well as hazardous medical devices. Training in the area of drug and medical devices is therefore necessary for staff of the Division of Environmental Health. Forged prescriptions, lack of accountability for controlled substances by businesses, and illegal dispensing of controlled substances are perceived to be significant problem;. however, because of the lack of human resources, only the most significant cases are pursued and investigated.

Guam is faced with the challenge of maintaining a health care system that will adequately meet the needs of a predominantly young and growing population. At the same time, it is also facing the added challenge of addressing the problems of the rapidly increasing number of older

people, forecast to increase from 3.9% of the total population in 1990 to 7.5% in 2010.

Guam sees significant opportunity to capitalize on the additional resources (funding, training, tools and incentives for adoption of Health IT and Health Information Exchange) through the various program s established by Office of the National Coordinator for Health Information Technology (ONC) in response to HITECH legislation and $1.6 Million in funding made available through the American Recovery and Reinvestment Act (ARRA). Guam's Strategic and Operational Plan (SOP) for Statewide Health Information Exchange was approved by the Office of the National Coordinator (ONC) in April 2010. As Guam implemented this approved plan, and its strategies remain consistent for the long-term, some adjustments have been made in short-term plans, in response to barriers encountered; these changes are summarized in Section 2 of this document, and described in further detail in other sections.

As proposed in the initial Strategic and Operational Plan which was approved in 2010, Guam intends to pursue a phased approach for the following strategies:

a. Governance through Guam eHealth Collaborative (GeHC), a public-private collaborative with oversight from the Office of the Governor and the Guam Department of Public Health, and leadership from appointed advisory council and professional staff.
b. Phased development and deployment of technical services to enable secure exchange and meaningful use of health information, beginning with Direct secure messaging capabilities enabled by a selected vendor, local management of digital certificates and access to information via a secure portal for authorized users. After a sufficient level of use to assure sustainability of these directed exchange services, GeHC will begin development and deployment of more robust query-based exchange infrastructure in later phases, including a master patient index, record locator service, and interfaces to clinical data repositories to enable population health management and analytics to achieve improved health outcomes, as well as improved quality and cost of health services.
c. Development and adoption of a framework to protect privacy and security through policies, procedures and infrastructure addressing information technology, information management, training and oversight for personnel and users, including scheduled and unscheduled audits.
d. Financial resources from a variety of sources (federal, state, and user-generated) adequate to support and sustain development, marketing, deployment and ongoing operations of the services needed to enable meaningful use of health information by providers, patients, public health and payers, including Medicaid. GeHC will consider customer demand, market competition, and financial viability for any services to be offered, as well as organizational capacity to manage financial and physical resources in accordance with generally-accepted accounting procedures, including auditing and reporting requirements.

e. Effective management of business and technical operations, including employed and contracted personnel qualified to manage projects, communications, finances, IT systems, and program evaluation in accordance with approved plans, policies and procedures.

2.0 SUMMARY OF CHANGES IN HIE STRATEGY, FROM INITIAL PLAN APPROVAL IN 2010 TO 2012 PLAN UPDATE

Domain/Sections	Short Description of Approved Portion of SOP that Grantee is Proposing to Change (include page numbers)	Proposed Changes	Reason for the Proposed Change	Budget Implications of Proposed Changes
Overall HIE Strategy including Phasing	See Technology and Financial Below			
Governance	NONE	N/A	N/A	NONE
Project Management Plan/Technology	Page 32 – 33 Section 7.0	Description of actual technology selected	Initial vendor selected, under-performance led to decision to transition to alternative vendors (Direct secure messaging capabilities, consulting services for project management and oversight)	NONE
Financial	Page 12 – 21 Section 5.0	Methodology and plan for assessing market for Direct secure messaging and other services	Viable plan for sustainability of HIE (intra- and inter-state)	NONE

Legal/Policy	XX	Framework for Protection of Privacy and Security	federal and state requirements to protect privacy and security of health information	NONE
Strategies for e-Prescribing	NONE	N/A	N/A	NONE
Strategies for Structured Lab Results Exchange	NONE	participation in lab exchange pilot	barriers encountered in enabling exchange with major lab provider	NONE
Strategies for Care Summary Exchange	NONE	N/A	N/A	NONE

3.0   Progress and Current Landscape for HIE, as of 12/31/2012

In accordance with the initial Strategic and Operational Plan which was approved in 2010, Guam has designated an HIT Coordinator from the Guam Department of Health, whose participation assures coordination with other state agencies, as well as communication and commitment from leaders in the public and private sector. Guam has established a public-private collaborative, the Guam eHealth Collaborative (GeHC), with a leadership board comprised of key stakeholders, and a small professional staff of 2: an HIE Program Director responsible for oversight of vendors and outreach to providers, and an administrative assistant / business manager who will begin work in January 2013 to manage funding and reporting requirements. An organizational chart and membership list is included in Appendix A of this document.

After a vendor selection process undertaken in 2011, a contract was executed with Apenimed to deploy and operate infrastructure to enable Direct Secure Messaging services, and its partner Hielix to provide project management and planning for financial sustainability. Apenimed began in November 2011 to deploy its Direct application, which was fully functional by February 2012. As of December 2012, the GeHC has signed up to 50 Direct users thus far. Guam has explored a Direct pilot with the Veterans Administration, and a lab pilot for exchange between Guam providers and a lab in Hawaii, a project which was highlighted at the 2012 ONC Annual meeting.

However, delays in implementation and constraints in personnel have led to slower adoption by providers than anticipated, resulting in delay of Guam's plan to initiate Phase II infrastructure development and creating challenges for financial viability and sustainability. GeHC is therefore considering transition to other vendors in 2013, and will work with experts from the State HIE Technical Assistance Program to assure seamless transition and financial viability of services for current and future users.   Timelines for vendor transition, sustainability planning and communications / outreach to users are detailed in the project management plan, included in Section 7 of this document.

Guam is committed to the protection of privacy and confidentiality for individuals whose information is exchanged within and outside of the Territory; GeHC has therefore developed a Privacy and Security Framework, which is described in Section 4 of this document, for consideration and adoption by its governing board. Policies which have been drafted for consideration and adoption are included in Appendix B of this document.

As of December 2012, funding support for GeHC is provided by federal and state sources, in accordance with the terms of the ONC State HIE Cooperative Agreement; however, recognizing that this funding will expire on September 30, 2013, GeHC has engaged consulting services from

HIElix, supplemented by technical assistance through the State HIE Technical Assistance Program, to better understand the various strategies undertaken by HIEs nationwide since the inception of national initiatives a decade ago, and to identify the key stakeholders in the market who should be contacted regarding their level of interest in various services that might be offered by GeHC, as well as the pricing thresholds which they might consider. A high-level description of our plan to sustain HIE through various policy and contractual levers, resulting in financially viable service offerings through GeHC, is described in the HIE Sustainability Plan which is included in Section 5 of this document.

Finally, GeHC understands the need to monitor and evaluate the success of GeHC, both as a requirement of the ONC State HIE Cooperative Agreement and as a mechanism to assure effective use of resources and continuous quality improvement in a rapidly-evolving market for health care and health information technology services. GeHC has increased its staff capacity to support the necessary administrative tasks and required reporting for elements as described in Appendix B and C. GeHC further intends to identify qualified resources to conduct program evaluation, who will begin no later than March 31, 2013 in order to collect and review data, and then report finding no later than September 15, 2013. Guam's approach and indicators for program evaluation is further detailed in Section 6 of this document.

4.0 PRIVACY AND SECURITY FRAMEWORK

As directed by the Governor's Executive Order designating the Guam eHealth Collaborative (GeHC) as the trusted source of health information for residents in Guam, GeHC is required to comply with the Health Information Portability and Accountability Act (HIPAA) regulations regarding the use and disclosure of protected health information (PHI). These regulations require Covered Entities and their Business Associates to implement administrative, physical and technical safeguards that ensure the confidentiality, integrity, and availability of electronic health information. These safeguards are designed to:

1. Ensure the confidentiality, integrity and availability of all ePHI which it creates, receives, maintains or transmits;
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information
3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted by the HIPAA Privacy Regulations; and
4. Ensure compliance with the HIPAA Security Regulations by its workforce.

Along with its phased approach to infrastructure development and deployment, GeHC has also elected to develop and implement its policies and procedures in an incremental fashion. In support of its phased strategy and initial offering of Direct secure messaging services, With support from its legal counsel, contracted consultant, and ONC's State HIE Technical Assistance Program, GeHC has drafted a limited set of core policies which support the exchange of clinical and administrative data for the purpose of treatment, payment and operations in accordance with the protocols defined by the Direct Trust community, and allowing access to the information by authorized users of the Guam HIE Web Portal. Following the successful implementation and sufficient adoption of Direct Secure Messaging services in Phase I in 2013, GeHC intends to develop and adopt further policies to support additional exchange capabilities, including nationwide exchange as a participant in the eHealth Exchange and a proposed provider directory which will be shared with Guam Medicaid.

 The GeHC Board will review and approve the core set of policies and procedures prior to March 31, 2013, when the Direct services will be activated by GeHC's vendor. These policies and procedures, currently in draft format, are included in Appendix B of this document.

GeHC intends to leverage the resources of the Guam Department of Health and the Bureau of Health Care Financing to identify an individual to be designated as the HIE Privacy Officer. The HIE Privacy Officer will be appointed in February 2013, and will consistently monitor, and periodically audit, privacy practices to ensure compliance with approved policies and procedures.

Because Guam has a relatively small number of providers, GeHC has elected to implement a Guam-based certificate authority to support the users of Direct Secure Messaging. The certificates will be issued and managed initially by GeHC staff, but Guam will consider linking the Guam certificate authority to the Federal Bridge certificate authority so as to allow exchange between local providers and federal agencies, including the Department of Defense and the Social Security Administration, which have significant presence locally.

GeHC has established contractual requirements for its vendors and suppliers, to maintain proper safeguards to protect the privacy and security of any information to which they might have access in the course of delivering any contracted services. These requirements are specified through Business Associate Agreements, which bind both GeHC and its vendors to comply with the requirements of Covered Entities which participate in exchange activities.

The GeHC will be a primary source of knowledge and information about health information technology for providers and consumers in Guam, and will work in collaboration with other Territorial, State and Federal programs, including the designated Regional Extension Center which is the University of Hawai'i, subcontractor to the Hawai'i Health Information Exchange. GeHC will implement a communication and education plan, to educate GeHC board members, staff and participants on the policies and procedures which are applicable to their respective roles.

5.0   PLAN FOR SUSTAINING HEALTH INFORMATION EXCHANGE

BACKGROUND

Guam has benefitted from the $1.6 Million funding allocation and technical assistance resources provided through the State HIE Cooperative Agreement Program with ONC, and have recognized that these resources will no longer be available after September 2013. GeHC wishes to leverage the investments made to date to continue and extend the exchange of health information within and outside the Territory. Therefore, Guam has begun establishing mechanisms to ensure that there are incentives for users to participate in the exchange of health information, and that there is sufficient market demand and revenue to sustain the operational costs for current and new services beyond 2013.

GeHC began the process of determining user demand and competitive market rates for services which might be offered in February 2012, when its contracted consultant compiled and analyzed the following:
- A review of relevant literature
- A review of funding strategies pursued by other HIE entities nationwide to generate both capital and operating revenue
- An analysis of local stakeholders likely to participate in health information exchange, and the potential value proposition for each of these stakeholder groups
- An analysis of risk for the long-term sustainability of an HIE entity in Guam

As a result of these analyses, GeHC has defined and adopted the following principles to assure sustainability:
- Communicate with and educate participants early and often regarding the value and benefits of HIE, recognizing that health information technology is an enabler for a broader vision to improve health outcomes, quality and cost.
- Create and foster trust among stakeholders to further the willingness to exchange healthcare information and data by protecting the privacy and confidentiality of individuals and the security of information, and by operating with transparency and accountability.
- Create value for each participant by articulating use cases, providing quality services and monitoring and reporting outcomes that are relevant and accurate.
- Ensure fair and equitable investment by stakeholders and users, to build and sustain HIE through financial and other contributions.
- Leverage collaborative partnerships (with the Regional Extension Center, Public Health, Medicaid, other states and territories, and private sector stakeholders) to share best

practices and lessons learned, and to leverage and share infrastructure to support common goals and use cases.

,

Assessing Customer Demand and Pricing for Current and Potential Service Offerings

Various funding options have been explored; after careful study, GeHC leaders have agreed to pursue the strategies described below. Our approach is based on the recognition that three key industry segments provide approximately equal contributions to sustainability:

1) the territorial government and several state agencies including Medicaid and Public Health;
2) payers; and
3) providers, including both hospitals and physicians.

Other stakeholders in the state include long-term care providers, labs, radiology, pharmacies, hospice, accountable care organizations, and other programs which may pay nominal fees for use of HIE services. Although these fees may not provide a major source of revenue, the ability to exchange health information with these health service providers is a significant incentive for the major stakeholders listed above, to improve coordination during transitions of care and thereby leading to improved outcomes, quality and cost.

1) Participation by Territorial Government and State Agencies, including Medicaid and Public Health

The Centers for Medicare and Medicaid Services (CMS) has allocated resources to promote adoption of EHRs and HIE through incentives for hospitals under the Medicaid EHR Incentives program, while providers can qualify for incentives under both Medicare and Medicaid EHR incentives programs. As of December 2012, 13 eligible providers had received a total of $222,919 through Medicare EHR Incentives Program payments, while no hospitals or providers had received payments through the Medicaid EHR Incentives program.

GeHC is collaborating with Guam Medicaid to strengthen its capacity to support providers to meet requirements for meaningful use of health information, as described in Guam's State Medicaid HIT Plan (SMHP). As work begins on Medicaid's Implementation Advanced Planning Document (IAPD), GeHC will support outreach, education and services to enable electronic exchange of information by eligible Medicaid providers with others via its Direct Secure Messaging offering. GeHC will work with Guam Medicaid to explore subsidies for early adopters for an initial period of time (between April 1, 2013 through August 31, 2013).

GeHC and Medicaid are also exploring the feasibility of a shared provider directory, which would be populated with the identifiers and contact information currently maintained manually by Guam Medicaid, but which would also include Direct addresses and security credentials issued by GeHC to allow routing of Direct Secure Messages via the Guam HIE Web Portal.

Medicaid has included an allocation for funding support in its budget for this service, beginning September 2013. This service could also be shared by Guam Department of Public Health, to support required reporting to public health and notifications and alerts from public health officials to providers and facilities. It is GeHC's intent to enable these capabilities before the end of 2013, and to determine costs and pricing models in the second quarter of 2013 so that users can be activated and revenue can be generated beginning October 1, 2013, at levels totaling approximately one-third of total revenue.

2) **Payers**

In addition to Medicaid, which serves approximately 8,000 individuals (5% of the total population), and TriCare which serves veterans and active duty military personnel, other health insurers in Guam include these four largest private insurers:
- Staywell
- TakeCare
- Calvos
- Netcare

According to an article published by Guam Business, annual premiums for these health insurers amount to between $150 Million to $250 Million annually. GeHC will explore with these payers the ways in which existing HIE infrastructure could be used to increase efficiency and reduce cost for eligibility verification, chart audits, and / or quality reporting by users, as well as an acceptable fee structure and timeline for these service offerings. It is anticipated that these services could be added in 2014, if market demand and revenue is sufficient to cover costs of providing those services.

GeHC will work in collaboration with the Guam Department of Revenue and Taxation, which received $1 Million through the Affordable Care Act to survey businesses in order to collect data on insured and uninsured employees, to understand the current landscape in the health insurance market, and to engage leaders from these organizations to explore their desire for services (shared provider directory, secure access to information via the Guam HIE portal, and / or Direct secure messaging) which might be offered to their personnel, members, and / or their network of providers by GeHC. GeHC will determine the cost for delivery of these services, as well as an acceptable fee structure, no later than June 30, 2013, so that users could be enrolled and revenue generated beginning October 1, 2013, at levels totaling approximately one-third of total revenue.

3) **Providers**

Because there are a relatively small number of providers in Guam, and because these providers suffer from severe financial constraints and lack of HIT / HIE expertise among their personnel, it is imperative that HIE infrastructure be as low-cost and easy-to-use as possible. GeHC's phased approach has enabled the most basic method of information exchange, offering security credentials, access to information via a secure web-based portal, and point-to-point secure messaging in compliance with Direct protocols. While these services have initially been offered at no cost to participants based in Guam, and will continue to be provided at no cost through Sept. 30, 2013, GeHC will begin to charge user fees as of October 1, 2013. These fees will be kept as low as possible, but must generate enough revenue to cover approximately one-third of the annual operating costs for this infrastructure.

Of the approximately 150 licensed providers in Guam, GeHC has targeted 300 users of HIE Phase I services by September 30, 2013. As Guam's only non-military hospital, Guam Memorial Hospital is also committed to use of the HIE services provided by GeHC, and has indicated an interest in Phase II services which would include query-based exchange and connectivity to the nationwide eHealth Exchange, which would most likely become operational in early 2014. GeHC will also engage with providers and their partners who are considering and / or forming collaboratives to support patient-centered medical homes and accountable care organizations, in order to understand how current and future HIE infrastructure can support new payment models, and the manner in which the cost of supporting HIE services can be covered. It is likely that these new models may not be initiated or operational until 2014 or later, but GeHC must be alert to the changes in the health care market may impact its assumptions and projections for financial sustainability.

4) Other Entities

Pending successful resolution of issues related to lab ordering and results delivery via Direct Secure Messaging, which are being addressed through Guam's participation with the highest-volume lab provider, Hawai'i-based Diagnostic Lab Services (DLS), in a Direct pilot through ONC, it is anticipated that DLS will begin paying for this service beginning in July 1, 2013, provided that GeHC can offer this service at a cost lower than DLS currently pays for maintaining interfaces and / or delivering results via a portal to Guam-based providers. GeHC will continue discussions with DLS to determine attractive pricing structure and to determine whether revenue will be sufficient to cover expenses for this service, noting that access to electronic lab results may be highly attractive to participating providers.

Since 2010, federal initiatives through the US Department of Health and Human Services have provided funding for the following:

- $1,020,098 from the Health Resources and Services Administration (HRSA) to expand capacity of federally-qualified health centers which provide preventive and primary care services to 13,947 individuals
- $1.5 Million from HRSA and the Administration for Children and Families (ACF) to establish a home visiting program to strengthen maternal, infant and early childhood health, educational and economic outcomes
- $1 Million through the Affordable Care Act to establish a health insurance exchange serving residents of Guam

Guam's HIT Coordinator is charged with the responsibility of coordinating with these various federally-funded programs, and with exploring opportunities to leverage these investments through alignment of policies, planning, technical infrastructure, personnel and budget allocations, so as to avoid duplication and competition, and to assure cost-effective sharing of services to the fullest extent possible. GeHC intends to work collaboratively with leaders of these programs and initiatives, to determine whether its current infrastructure and services could offer advantages for communication and coordination among participants and staff of these services. Possible options for shared infrastructure include management of security credentials and digital certificates, access to information via a secure portal, Direct secure messaging, and a common provider directory,   In March and April 2013, GeHC will engage these potential partners in discussions with the goal of increasing the number of customers for its service offering in 2013, and to determine the pricing models and thresholds which allow for sufficient adoption to assure financial sustainability in future years.

All of these current and future service offerings will be explored by GeHC, using contracted services from qualified consultant with relevant expertise and knowledge of Guam's local market. GeHC intends to execute a contract for this support, which would begin no later than April 1, 2013 and result in a report and recommendations to the GeHC board no later than June 30, 2013. This will occur in conjunction with the planning for Phase II infrastructure development and deployment, which is anticipated to begin in Q3 of 2013 and to be operational by the end of December 2013.

GeHC will also develop the infrastructure for handling invoices and payments for services to its customers, as well as the administration of financial reporting and auditing in accordance with Generally-Accepted Accounting Principles (GAAP), as required of organizations receiving public funding from federal, state and other sources. Infrastructure requirements include, at a minimum, an accounting software package and personnel trained to manage financial resources appropriately, to be in place prior to June 30, 2013. GeHC's board will designate a Treasurer, who will be accountable to the GeHC board and funders for regular reports and audits; funding will be allocated from GeHC's budget to contract for an independent auditor to conduct an annual audit in compliance with A-133 requirements for organizations which

receive more than $500,000 in state and / or federal funds a given fiscal year, should this apply to GeHC's circumstances.

STATE POLICY LEVERS USED TO ENCOURAGE ADOPTION AND USAGE

As of December 2012, Guam had not proposed or approved policies to require adoption of electronic health records (EHR) or participation in health information exchange (HIE). However, Guam has received $700,000 in funding through the Affordable Care Act, which has been used to create a Prevention and Public Health fund which is directed to create effective policies which prevent illness and improve health in Guam, its communities and nationwide. GeHC intends to partner with leaders of this initiative to draft and gain approval for policies which advance the following strategies:

- licensure and accreditation requirements: for pharmacies, to increase the rates of participation in electronic e-prescribing and prescription drug monitoring programs; for labs, to increase the percentage of participation in electronic ordering and results delivery; for hospitals, to increase requirements for review of medication lists, notifications to ambulatory providers upon discharge from inpatient and / or emergency department visits; for clinicians, to provide patient records when making a referral to other health professionals; and for health insurance providers, to increase requirements for portability and affordability for members.
- value-based purchasing: for public payers (Medicaid, Medicare and government employee benefits programs), contractual requirements that HIT and HIE capabilities be required of providers desiring to participate in the network of contracted providers delivering services to members.
- Public health reporting: for healthcare service providers (ambulatory care, clinics, hospitals, behavioral health, long-term care facilities, pharmacies, and labs) to submit required reports electronically to public health systems as those become electronically enabled to receive these reports: immunization and cancer registries, infectious disease and other bio-surveillance programs, labs, and environmental health programs. Similar to other states, the Guam Department of Public Health could designate GeHC as the single or preferred point of access for sending and receiving information between public health officials and health care service providers in Guam.
- Capabilities to increase protections for privacy and security: legislation and / or administrative regulations requiring digital certificates and security credentials for any individual (clinician, patient, provider support staff, researcher, system administrator, vendor, auditor, or compliance officer) seeking access to electronic health information at a level that meets or exceeds HIPAA requirements. GeHC could collaborate with the Regional Extension Center to educate and increase awareness among participants, to conduct risk assessments, and also provide services such as issuance and management of digital certificates, access to electronic information via a secure portal, and reports

documenting the disclosure of information and the level of compliance with laws and policies.

FIVE-YEAR REVENUE AND EXPENSE PROJECTIONS

Assumptions
General
- Sustainability is targeted for State Fiscal Year 16 (SFY16) beginning July 1, 2015

Revenue
- Federal funding will be accessible through the ONC State HIE Cooperative Agreement, totaling approximately $750,000 from January through September 2013.
- Allocations of financial and in-kind contributions will be included in the general fund of the Guam Department of Health, to support the cost of development and Phase I and Phase II services. Beginning in FY 2016, financial contributions to GeHC from the Guam Department of Health will be budgeted in accordance with the mutually agreeable pricing and timeframes established for public health consumers of information and for the services required to support public health use cases.
- Guam Medicaid will allocate financial and in-kind contributions to support the costs of Phase I and Phase II services, beginning in October 2013. Allocations will be proportionate to the percentage of Guam's population who are served by Medicaid (5%), and will support meaningful use and quality reporting by Medicaid-eligible providers, as well as member access to health information. Funding allocations will be included in the State Medicaid HIT Plan (SMHP), and implemented in accordance with the approved Implementation-Advanced Planning Document (I-APD).
- User fees will take effect October 1, 2013, in accordance with the mutually agreeable pricing and timeframes established for providers, labs, payers, patients and other users.
- HIE revenues will cover all HIE expenses by State Fiscal Year 2016 and provide a reasonable, positive operating margin
- Participation fees will be structured as follows:
    - SFY12   No fees
    - SFY13   50% of the SFY16 sustainability requirement
    - SFY14   100% of the SFY16 sustainability requirement
    - SFY15   100% of the SFY16 sustainability requirement
    - SFY16   100% of the SFY16 sustainability requirement
- Proposed Fee Structure (to be explored with prospective customers and adjusted according to customer demand, perceived value and market competition):
    - Hospitals   Flat fee for Guam Memorial and Medical City

- o   Provider Practices $400 per physician
- o   Payers $ 1.50 per member
- o   Long-Term Care $250 per facility
- o   Pharmacies $250 per location
- o   Labs $500 per lab
- o   Radiology $250 per location
- o   Home Health Care $250 per facility
- o   Other $250 per facility
- Fees will be evaluated, and may be adjusted from time-to-time, based on:
  - o   the previous year's expenses, actual HIE participation rates, and actual revenues
  - o   the upcoming year's projected expenses, projected HIE participation, and projected revenue
  - o   changes in HIE services (e.g., for new services or additional functionality)
  - o   estimated costs to perform desired services (e.g., for new services or additional functionality)
- Adoption rates in SFY16 are as follows:
  - o   100% for hospitals
  - o   75% for physicians
  - o   75% for payer members
- Local public health departments that offer clinic services are included within the Provider Practice Fee structure
- Annual margin targets should be approximately equal to two months of expenses (17%).

Expense
- Staffing includes the following positions:
  - o   Executive Director (SFY12)
  - o   Technology Support (SFY12)
  - o   Administrative / Bookkeeping (SFY13)
  - o   Privacy Officer / Legal Counsel (SFY13).

Expenses related to the operational costs of the HIE include the following:
- A.   HIE Infrastructure and Services
  - Non-Recurring Costs (i.e., project initiation and planning; software licensing; install, testing and implementation)
  - On-Going Operational Costs (i.e., data hosting; portal and secure messaging; direct connection; software maintenance, and professional services for project management, business development, communications / outreach, policy development, audit, etc.);
- B.   Other Expenses

- These expenses include: legal, program evaluation, travel, office equipment and supplies, insurance, Executive Committee and Advisory Council meeting expenses

sample spreadsheet for projecting income and expense

Revenue / Stakeholder	Count FFY12	FFY13	FFY14	FFY15	FFY16	Rate FFY12	FFY13	FFY14	FFY15	FFY16	Annual FFY12	FFY13	FFY14	FFY15	FFY16
Federal Funds	1	1	1	1	1	843,119	201,374	$105,688	-	-	$ 843,119	$ 201,374	$ 105,688	$ -	$ -
Veterans Administration	1	1	1	1	1	30,000	159,000	$25,000	25,000	25,000	$ 30,000	$ 159,000	$ 25,000	$ 25,000	$ 25,000
State Direct Appropriation	1	1	1	1	1	-	-	$ -	-	-	$ -	$ -	$ -	$ -	$ -
Hospitals and Health Systems						Rate Per Hospital									
Guam Memorial	1	1	1	1	1	20,000	20,000	$ 20,000	20,000	20,000	$ -	$ 10,000	$ 20,000	$ 20,000	$ 20,000
Medical City	0	0	1	1	1	40,000	40,000	$ 40,000	40,000	40,000	$ -	$ 20,000	$ 40,000	$ 40,000	$ 40,000
Provider Practices		Cumulative Number of Provider				Rate per Provider									
Birthing Center	0	0	0	0	0						$ -	$ -	$ -	$ -	$ -
American Medical Clinic	0	0	0	0	0						$ -	$ -	$ -	$ -	$ -
Med First Clinic	0	0	0	0	0						$ -	$ -	$ -	$ -	$ -
Seventh Day Adventist	0	0	0	0	0						$ -	$ -	$ -	$ -	$ -
Physicians	250	250	250	250	250	400	400	400	400	400	$ -	$ 50,000	$ 100,000	$ 100,000	$ 100,000
Government Agencies		Number of Agencies				Rate per Agency									
Public Health	3	3	3	3	3	10,000	10,000	10,000	10,000	10,000	$ -	$ 15,000	$ 30,000	$ 30,000	$ 30,000
Corrections	1	1	1	1	1	10,000	10,000	10,000	10,000	10,000	$ -	$ 5,000	$ 10,000	$ 10,000	$ 10,000
Worker Compensation	1	1	1	1	1	10,000	10,000	10,000	10,000	10,000	$ -	$ 5,000	$ 10,000	$ 10,000	$ 10,000
Payers		Cumulative Number of Members				Rate per Covered Life									
Calvos SelectCare	0	32,000	32,000	32,000	32,000	1.50	1.50	1.50	1.50	1.50	$ -	$ 24,000	$ 48,000	$ 48,000	$ 48,000
Medicaid	0	50,000	50,000	50,000	50,000	1.50	1.50	1.50	1.50	1.50	$ -	$ 37,500	$ 75,000	$ 75,000	$ 75,000
Net Care	0	15,000	15,000	15,000	15,000	1.50	1.50	1.50	1.50	1.50	$ -	$ 11,250	$ 22,500	$ 22,500	$ 22,500
Stay Well	0	15,000	15,000	15,000	15,000	1.50	1.50	1.50	1.50	1.50	$ -	$ 11,250	$ 22,500	$ 22,500	$ 22,500
TakeCare	0	25,000	25,000	25,000	25,000	1.50	1.50	1.50	1.50	1.50	$ -	$ 18,750	$ 37,500	$ 37,500	$ 37,500
Third Party Admin / Self-Insured	0	12,000	12,000	12,000	12,000	1.50	1.50	1.50	1.50	1.50	$ -	$ 9,000	$ 18,000	$ 18,000	$ 18,000
Other Providers		Cumulative Number of Entities				Rate per Entity									
Long-Term Care	0	12	12	12	12	250	250	250	250	250	$ -	$ 1,500	$ 3,000	$ 3,000	$ 3,000
Pharmacies	0	36	36	36	36	250	250	250	250	250	$ -	$ 4,500	$ 9,000	$ 9,000	$ 9,000
Labs	0	4	4	4	4	500	500	500	500	500	$ -	$ 1,000	$ 2,000	$ 2,000	$ 2,000
Radiology	0	2	2	2	2	250	250	250	250	250	$ -	$ 250	$ 500	$ 500	$ 500
Home Health Care	0	5	5	5	5	250	250	250	250	250	$ -	$ 625	$ 1,250	$ 1,250	$ 1,250
Grants	0	0	1	1	2	-	50,000	50,000	50,000	50,000	$ -	$ -	$ 50,000	$ 50,000	$ 100,000
Total Revenue											$ 873,119	$ 584,999	$ 629,938	$ 524,250	$ 574,250

Expense						Rate FFY12	FFY13	FFY14	FFY15	FFY16	Annual FFY12	FFY13	FFY14	FFY15	FFY16
Core Infrastructure						591,144	105,688	$ -	-	-	$ 591,144	$ 105,688	$ -	$ -	$ -
Professional Services						-	75,000	$ -	-	-	$ -	$ 75,000	$ -	$ -	$ -
Subscription and Maintenance Fees						-	-	$150,000	150,000	150,000	$ -	$ -	$ 150,000	$ 150,000	$ 150,000
GeHC Staffing															
Personnel						133,900	170,362	$187,398	206,138	226,752	$ 133,900	$ 170,362	$ 187,398	$ 206,138	$ 226,752
Fringe Benefits						55,157	71,027	$ 78,130	85,943	94,537	$ 55,157	$ 71,027	$ 78,130	$ 85,943	$ 94,537
Travel						46,618	46,588	$ 15,000	15,000	15,000	$ 46,618	$ 46,588	$ 15,000	$ 15,000	$ 15,000
Supplies						6,000	6,180	$ 6,798	7,478	8,226	$ 6,000	$ 6,180	$ 6,798	$ 7,478	$ 8,226
Equipment						10,300	6,484	$ 7,132	7,846	8,630	$ 10,300	$ 6,484	$ 7,132	$ 7,846	$ 8,630
Unanticipated Expenses						30,000	30,000	$ 30,000	25,000	25,000	$ 30,000	$ 30,000	$ 30,000	$ 25,000	$ 25,000
Total Expense											$ 873,119	$ 511,329	$ 474,458	$ 497,404	$ 528,145
Margin											$ -	$ 73,670	$ 155,480	$ 26,846	$ 46,105
Margin %											0.00%	12.59%	24.68%	5.12%	8.03%

22

6.0   PROGRAM EVALUATION

Background

In 2009, the Guam eHealth Collaborative (GeHC) was established to plan, implement, and operate health information exchange (HIE) for the territory. The GeHC, comprised of 15 stakeholder members representing various public and private agencies, was formed to facilitate the adoption and use of health information technology and exchange of health information. The GeHC began implementation of the HIE to allow providers to electronically connect to other participating members for the exchange of healthcare data in the fall of 2011.

In first quarter of 2013, the GeHC will form an evaluation team to measure progress in Guam. The evaluation team will conduct a program evaluation beginning in April 2013, resulting in a final report by August 31, 2013, assessing the effectiveness of GeHC's Phase I service offering. The program evaluation will examine a number of quantitative metrics, using a set of qualitative and quantitative assessment tools designed to measure the process and outcomes of the Guam HIE, provider adoption, and value to users. In general, evaluation efforts will include a focus on adoption/utilization, effectiveness, barriers/vulnerabilities, and recommendations for system and program improvement. All collected information will be analyzed to (1) describe Guam's approaches and strategies, (2) indicate how they intend to impact HIE performance in each of the program priority areas (i.e., labs participating in delivering e-structured lab results, pharmacies participating in e-prescribing, providers exchanging summary of care records), (3) measure levels of progress achieved (e.g., how exchange has increased), (4) delineate factors that facilitated and inhibited progress, (5) determination of value, and (6) describe lessons learned for Guam which can guide further development and continuous improvement processes.

Evaluation Format

The following areas are considered critical for conducting the program evaluation program in Guam.

PIN 002 Priority 1	Aim and Research Question	Research Design and Methods
Goal: To facilitate exchange of electronic prescribing and payment .	**Aim:** Analyze HIE performance in transmission and execution of e-Prescribing . **Research question:** What percentage of licensed pharmacies can send or receive any electronic new prescription, refill request, or refill response	**Study design:** Retrospective data analysis. **Study population:** licensed pharmacies operating in the state (per NCPDP). **Data sources and data collection methods:** NCPDP data

	message in December of the previous year?	**Data Analysis:** Quantitative analysis of December 2011 data of NCPDP data. Transactions related to exchange of eligibility details.
	PIN requirements: What does the HIE intend to accomplish? How much progress has been made? What enabled or prevented this progress? What lessons have been learned?	• Number of transactions on formulary and benefits information. • Number of transactions related to medication history. • Number of transactions on fill status notifications. • Number of ambulatory providers ePrescribing. • Number of hospitals ePrescribing. • Number of hospitals using only CPOE for medication orders. • Number of pharmacies ePrescribing.

Pin 002 Priorities 2 and 3	Aim and Research Question	Research Design and Methods
Goal: To facilitate laboratories participation using electronic structured lab results to improve care delivery and reduce duplicative order testing.	**Aim:** Analyze HIE performance in electronic clinical laboratory ordering and results delivery. **Research question:** What percentage of labs sending electronic lab results to providers in a structured format? **PIN requirements:** What does the HIE intend to accomplish? How much progress has been made? What enabled or prevented this progress? What lessons have been learned?	**Study design:** State census of clinical labs. ONC will provide sample instrument. **Study population:** Hospital and independent clinical laboratories that respond to census. **Data sources and data collection methods:** CLIA OSCAR database including DLS. USPS mailed questionnaire and web-based questionnaire. Survey: • Does the lab use electronic transport methods to receive test orders? • Total number of billable tests

		received by your lab?
		• Capable of sending lab results in structured format?
		• Do the lab results automatically upload to the medical record?
		• Percentage of lab results sent to an EHR?
		• Percentage of results sent outside following LOINC standards?
		• Have you implemented the LRI guide for lab results format?
		• Which HL7 message standards are currently in use?
		Data Analysis: Quantitative analysis of survey data to assess use of standards.

Pin 002 Priority 4	Aim and Research Question	Research Design and Methods
Goal: To enable hospitals exchanging care summary to support patient transitions and meet meaningful use requirements.	**Aim:** Identify and understand how the engagement of stakeholders support the HIE strategy to increase the exchange of admission, discharge and transfer care summaries. **Research question:** What percentage of hospitals are sharing electronic care summaries with a.) Unaffiliated hospitals and b.) Unaffiliated providers. **PIN requirements:** What does the HIE intend to accomplish?	**Study design:** Census. **Study population:** Non-federal acute care hospitals responding to AHA HIT supplemental survey. **Data sources and data collection methods:** AHA HIT supplemental survey results provided by ONC. **Data Analysis:** Articulate the mechanisms by which the program component results in the intended outcome. • Has provider to provider messaging been successfully piloted? Quantify. • Number of CCDs transmitted by provider type.

	How much progress has been made? What enabled or prevented this progress? What lessons have been learned?	• Give evidence that HIE supports meaningful use measures.

PIN 002 Priority 5	Aim and Research Question	Research Design and Methods
Goal: To enable providers exchanging care summary to support patient transitions and meet meaningful use requirements.	**Aim:** To assess how engagement with stakeholders supports our strategy to increase the exchange of admission, discharge and transfer care summaries? **Research question:** What percentage of ambulatory providers electronically share care summaries with other providers? **PIN requirements:** What does the HIE intend to accomplish? How much progress has been made? What enabled or prevented this progress? What lessons have been learned?	**Study design:** Survey. **Study population:** Ambulatory care, office based physicians responding to National Ambulatory Medical Care Survey. **Data sources and data collection methods:** National Ambulatory Medical Care Survey (NAMCS) Electronic Medical Records (EMR) Supplement (also known as National Electronic Health Records Survey). Results provided by ONC. **Data Analysis:** Has provider to provider messaging been successfully piloted? Quantify. • Number of CCDs transmitted by provider type. • Give evidence that HIE supports meaningful use measures. • Number of transmissions related to reporting of clinical quality data to CMS or state. • Number of transmissions supporting ambulatory clinical quality measures. • Number of transactions supporting hospital clinical

		quality measures. • Reporting related to additional quality of care metrics.

PIN 002 Priority 6	Aim and Research Question	Research Design and Methods
Goal: To facilitate public health reporting of laboratory results.	**Aim:** Analyze HIE ability to transmit electronic data to public health agencies. **Research question:** Does the HIE support public health receiving ELR data produced by EHRs or other electronic sources in HL7 2.5.1 format with LOINC and SNOMED? **PIN requirements:** What does the HIE intend to accomplish? How much progress has been made? What enabled or prevented this progress? What lessons have been learned?	**Study design:** Prospective telephone assessment **Study population:** All public health agencies within HIE **Data sources and data collection methods:** Public health information technology specialist telephone interview. **Data Analysis:** binary probability model Yes or NO. Articulate the mechanisms by which the program component results in the intended outcome.

PIN 002 Priority 7	Aim and Research Question	Research Design and Methods
Goal: To facilitate public health reporting of immunization records.	**Aim:** Analyze HIE ability to transmit electronic data to public health agencies. **Research question:** Does the HIE support public health receiving immunization registries receiving electronic immunization data produced by EHRs in HL7 2.3.1 or 2.5.1 formats using CVX codes. **PIN requirements:**	**Study design:** Prospective telephone assessment **Study population:** All public health agencies within HIE **Data sources and data collection methods:** Public health information technology specialist telephone interview. **Data Analysis:** binary probability model, Yes or NO. Articulate the

	What does the HIE intend to accomplish? How much progress has been made? What enabled or prevented this progress? What lessons have been learned?	mechanisms by which the program component results in the intended outcome. • Transactions on query for immunization history and delivery (request and/or receive). • Transactions supporting decision forecasting (decision support.

PIN 002 Priority 8	Aim and Research Question	Research Design and Methods
Goal: To facilitate public health reporting of syndromic surveillance by hospitals.	**Aim:** Analyze HIE ability to transmit electronic data to public health agencies. **Research question:** Does the HIE support public health receiving electronic syndromic surveillance data from hospitals produced by EHRs in HL7 2.3.1 or 2.5.1 formats using CDC reference guides. **PIN requirements:** What does the HIE intend to accomplish? How much progress has been made? What enabled or prevented this progress? What lessons have been learned?	**Study design:** Prospective telephone assessment **Study population:** All public health agencies and a cross section of member entities **Data sources and data collection methods:** Public health information technology specialist telephone interview. **Data Analysis:** binary probability model Yes or NO. Articulate the mechanisms by which the program component results in the intended outcome. • Transactions of electronic surveillance data. • Transmission of electronic data on reportable disease conditions to public health agencies.

PIN 002 Priority 9	Aim and Research Question	Research Design and Methods
Goal: To facilitate public health reporting of syndromic surveillance by ambulatory providers.	**Aim:** Analyze HIE ability to transmit electronic data to public health agencies.	**Study design:** Prospective telephone assessment **Study population:** All public

	Research question: Does the HIE support public health receiving electronic syndromic surveillance ambulatory data produced by EHRs in HL7 2.3.1 or 2.5.1 formats.	health agencies and a cross section of CMS EHR incentive program providers.
		Data sources and data collection methods: Public health information technology specialist telephone interview.
	PIN requirements: What does the HIE intend to accomplish? How much progress has been made? What enabled or prevented this progress? What lessons have been learned?	**Data Analysis:** binary probability model, Yes or NO. Articulate the mechanisms by which the program component results in the intended outcome.
		• Transactions of electronic surveillance data.
		• Transmission of electronic data on reportable disease conditions to public health agencies.

Additional Research Question	Aim and Research Question	Research Design and Methods
Goal: To build strong collaboration between HIE stakeholders.	**Aim:** To perform an impact assessment on care transitions, patient safety and duplicative order testing.	**Study design:** Survey stakeholder organizations using a Likert scale qualitative questionnaire to evaluate governance effectiveness.
.	**Research question:** Has the incidence of duplicative order testing and patient incident (never events) reports and hospital readmissions been reduced for entities enrolled in the HIE?	**Study population** Interview with HIE key stakeholders using a structured questionnaire.
		Data sources and data collection methods: CMS statistics and online survey with key stakeholders.
	PIN requirements: What does the HIE intend to accomplish? How much progress has been made? What enabled or prevented this	**Data Analysis:** trend reporting of quantitative data and qualitative analysis of survey responses. Articulate the

| | progress?
What lessons have been learned? | mechanisms by which the program component results in the intended outcome.
• Has the core HIE infrastructure been successfully pilot tested?
• Quantify the number and type of participation interest forms received.
• Report the number and cause of unplanned HIE downtimes.
• List the number of teaching aids available to providers including toolkits, implementation guides, manuals and FAQs. |

Additional Research Question	Aim and Research Question	Research Design and Methods
Goal: To demonstrate the continued expansion of the HIE utilization.	**Aim:** To assess the adoption and use of the HIE. **Research question:** Is the adoption of HIE progressing? What modifications should be made to the implementation? **PIN requirements:** What does the HIE intend to accomplish? How much progress has been made? What enabled or prevented this progress? What lessons have been learned?	**Study design:** Retrospective data collection on HIE activity. **Study population:** HIE participants. **Data sources and data collection methods:** HIE database administrative functions. Survey of REC and Medicaid EHR Incentive Program providers, hospitals and other care providers**.** **Data Analysis:** Quantitative analysis displayed in graphic format and qualitative survey report. Adoption rates by month for each of the following entities: • Physicians • Hospitals • Clinics • State Agencies

		• Others
		Measuring the following:
		• Number of unique logons per day
		• Number of patient records accessed per day
		• How users are accessing applications
		• Application responsiveness
		• Usage trending.

Additional Research Question	Aim and Research Question	Research Design and Methods
Goal: To maintain an effective governance model for statewide HIE.	**Aim:** To ascertain the governance model effectiveness. **Research question:** Does the HIE represent all stakeholder and guide the decision making? **PIN requirements:** What does the HIE intend to accomplish? How much progress has been made? What enabled or prevented this progress? What lessons have been learned?	**Study design:** Prospective survey **Study population:** HIE stakeholders **Data sources and data collection methods:** structured interviews with key HIE stakeholders including State CIO, Medicaid, ND-HIN members, REC, hospital association, and medical associations. **Data Analysis:** qualitative survey report. Articulate the mechanisms by which the program component results in the intended outcome. • Are stakeholders paying for use? • Has the HIE completed an annual Business and Financial Sustainability Report and shared it with stakeholders? • Does the HIE have an approved evaluation plan? • What data has been collected, complied and

		reported?
		• Are there approved policies and procedures regarding transmission of PHI?
		• Are there audit trails?

7.0 PROJECT MANAGEMENT PLAN AS OF 1/15/2013
7.1 PURPOSE OF THIS DOCUMENT

The purpose of the project plan is to define the project scope, schedule, budget, and quality expectations of the project, and to provide a comprehensive strategy for managing the project.

7.2 BACKGROUND

Guam is a participant in the United States Department of Health and Human Services Cooperative Agreement Program. Beginning in 2009, Guam has been actively working towards the development of an operational Health Information Exchange (HIE). In 2010, Guam wrote and submitted its Strategic and Operational Plan for HIE. The plan was submitted in September 2010 and approved in April 2011. Following the approved plan, Direct was implemented in late 2011 and was fully operat6ional in February 2012.

Guam's current HIE vendor has failed to satisfactorily fulfill its commitment to Guam regarding the building of an HIE infrastructure. Therefore, the Guan HIE Governing Board (Guam eHealth Health Collaborative – GeHC) has decided to replace the current HIE vendor. The strategy developed by the GeHC is to pursue a two pronged strategy for finding a replacement infrastructure vendor for its HIE. These two strategies will be pursued on parallel paths and concurrently.

The first strategy is to consider partnering with another state that has a fully operational HIE infrastructure. The intent is to find a suitable partner, negotiate a mutually beneficial contract and use the partner states HIE infrastructure to manage the Guam HIE. The GeHC is currently looking at five different potential including:
- Alaska
- Community Health Information Collaborative (CHIC) – The state HIE for Minnesota
- Delaware
- Hawaii
- Oregon

The second strategy is to identify a new infrastructure vendor using an RFP process. GeHC will follow the normal Guam procurement process to write the RFP, solicit responses, review and analyze the response, select a preferred vendor and negotiate the final contract.

The results of this process will converge in a timely manner to provide the GeHC with sufficient information to select the HIE infrastructure solution to provides Guam with the highest quality and lowest priced HIE.

7.3 PROJECT PURPOSE

Through the leadership of the GeHC, the Territory will replace the current HIE infrastructure and implement a fully functioning, sustainable health information network/exchange to be accessed by qualified organizations representing providers, physicians, hospitals, other health care organizations, and consumers.

7.4   PROJECT ASSUMPTIONS AND CONSTRAINTS

7.4.1   Assumptions

The project has the following assumptions:
- Resources will be available as defined in the project plan
- The required scope can be accomplished within the constraint of the appropriated funding
- Contract approximate start date is January 2013
- The approximate end date for the selection of a solution is June 2013
- The implementation of the selected solution is October 2013.
- Full operation of the Guam HIE will be completed by December 2013
- The GeHC will need significant outside consulting assistance to accomplish all of the required tasks as outlined in the project plan

7.4.2   Constraints

The project has the following constraints (restrictions or limitations either internal or external to the project):

- The budget for completing the required tasks is limited. Therefore, the GeHC will need to maintain tight control over the process.

- The providers currently using Direct services will lose service during the transition process. Therefore, they will need personal attention and management throughout this project to keep and maintain their interest in health information exchange

7.5   PROJECT APPROACH

In order to best accomplish the project's objectives, the GeHC will implement a project management approach based on industry standards and best practices, which is tailored to the specific needs of the project. The GeHC utilizes industry standards and best practices in performing its tasks, leveraging Project Management Body of Knowledge (PMBOK) for project management practices, and other industry standards from entities such as the Carnegie Mellon University and the Software Engineering Institute.

Using the PMBOK as a standard, The GeHC will manage the project along the eight core project management processes:
    Integration management
    Scope management
    Time management
    Cost management
    Quality management
    Human resource management
    Communications management
    Risk management

From a project protocol perspective GeHC will employ protocols based on the best practices found in the PMBOK. These include processes for communication and status reporting, risk and issue management, escalation and resolution, human resource and contract management and other contract control processes.

8.0   Governance

Governance identifies the key governance roles and responsibilities for the project. In addition to documenting the stakeholders involved in managing the project, this governance section covers who is responsible for approving project documents, who approves deliverables and who makes the final decision to accept the recommendations of the Guam HIE Director for a new solution. The escalation process for issues will also be defined.

The objective of this section is to detail the structure of the project organization, and the methods by which it reaches official decisions and carries out regular business. This ensures commitment and effective management of the project in order to:

- Ensure the project remains on course to deliver a new HIE infrastructure solution for the Guam HIE

- Approve all major deliverables

- Authorize deviations through integrated change control

- Authorize the negotiations for the recommended solution

- Approve the negotiated agreement for the new HIE infrastructure

- Ensure communication between the GeHC and providers in Guam is effective and consistent

8.1   AUTHORITY

The Guam eHealth Collaborative operates under the authority of an Executive Order from the Governor of the Territory of Guam. A copy of that order is included below.

Governors Executive Order

A. The Bureau of Information Technology and its Director shall be the "State Designated Agency" for all matters related to the Office of the National Coordinator, the exchange of healthcare data and information and the "Cooperative Agreement Program";

B. The GeHC shall provide guidance and coordination of electronic health information exchange and related efforts and promote engagement of health care providers, health care systems, and consumers among others;

C. The GeHC shall develop a plan to implement Health Information Exchange (HIE) considering ways to advance the adoption of electronic information technology, identifying opportunities for partnerships, incorporating national standard setting

organization recommendations for the secure exchange of patient healthcare data and information;

D. The GeHC shall promote the public good by ensuring an equitable and ethical approach to healthcare data and information exchange for the improvement of health care in Guam;

E. The GeHC shall encourage collaboration and facilitate a standardized approach to interoperable exchange of healthcare information in Guam and the region;

F. The GeHC shall recommend and implement policy that will advance the exchange of healthcare data and information in Guam while protecting the privacy and security of citizens' private health information;

G. The GeHC shall leverage existing healthcare exchange initiatives in Guam and proactively seek opportunities to utilize HIE for the betterment of Guam's health care system;

H. The GeHC shall consist of no more than 15 members appointed by the Governor. The GeHC shall be composed of the Agency Head or a representative from:
    1. Department of Public Health & Social Services
    2. Guam Memorial Hospital Authority
    3. Department of Mental Health & Substance Abuse
    4. Bureau of Information Technology
    5. Guam Community College
    6. Guam Medical Association
    7. Guam Medical Society
    8. Guam Nursing Association
    9. Guam Pharmacists Association
    10. Guam Legislature
    11. Guam Dental Association
    12. University of Guam
    13. Health Insurance Company
    14. Chamber of Commerce
    15. Representative identified by the Collaborative

I. The GeHC shall meet regularly as determined by the GeHC and conduct all necessary business activities to satisfy the requirements of this Executive Order. Action shall require an affirmative vote of a quorum of the appointed members to be binding;

J. The GeHC shall have the following specific enumerated powers:
    1. Development and adoption of an annual balanced budget for operations
    2. Hire an Executive Director and staff to enable the Guam Health Information Exchange to conduct normal and necessary business activities
    3. Determine and implement products and services as required for exchanging healthcare information and that provide funding for Health Information Exchange in Guam
    4. Enter into contracts with outside vendors to supply products and services to the GeHC as required for the normal and necessary conduct of business activities

5. Establish reasonable fees and charges for services and receive and disburse payments from those fess as required for the normal and necessary conduct of business activities
6. Create an account for the deposit of fees, charges, and grants and for the normal and necessary transaction of business following the accepted procedures for the Territory of Guam
7. Apply for and accept grants to establish, expand, or otherwise improve services
8. Determine if working with other states and territories will assist in providing healthcare information exchange services at a reduced cost to Guam. If so, the GeHC shall actively pursue and execute contracts to establish working relationship with other states and territories
9. Recommend legislative action to the Governor's office to enable the exchange of healthcare information in Guam
10. Establish policies and procedures for the normal and necessary conduct of business activities and the exchange of healthcare data and information
11. Recommend enforcement actions to ensure that providers in Guam act in the public interest without causing a disruption in healthcare information exchange services
12. Hold public hearings that provide an adequate opportunity for participating providers and entities as well as consumers the chance to provide feedback and recommendations on various GeHC activities including but not limited to fees and charges, budgets, policies and procedures, enforcement activities and grant applications

K. The GeHC shall provide updates to the Lieutenant Governor, including an annual written report on plans, activities, accomplishments and recommendations for healthcare information exchange in Guam;
L. The GeHC shall promote education and engagement among stakeholders to facilitate the successful implementation of health information exchange;
M. The GeHC shall further public and private partnerships for the development of an island-wide health information exchange infrastructure; and
N. The GeHC shall encourage Health Information Exchange initiatives to connect at the local, regional, and national level.

8.2 Staffing Plan

The Guam will operate with a team of three individuals. The Guam eHealth Collaborative (GeHC) has hired two positions to support the activities of the HIE Director.

The Guam HIE Director is a member of the Governors Cabinet and is also the Guam CIO. His responsibilities include:

- Manage the overall operation of the Guam HIE
- Manage the GeHC Board of Directors
- Financial management of the HIE including securing the funding needed for sustainability

- Legal and Policy formation including privacy and security issues
- Press relations in Guam

Position 1 – Technical Support

This position is responsible for the following activities:

- Recruit stakeholders for participation in the HIE
- Provide technical support for the HIE operations
- Work with stakeholders on technical issues
- Offer education to stakeholders on HIE capabilities
- Work with the HIE Director to resolve technical issues
- Consumer education

Position 3 – Administrative/Financial Support

This position will be hired in January 2013 and will be responsible for the following activities:

- Provide administrative support to the HIE Director and GeHC Board of Directors
- Manage the financial matters of the HIE including budgeting, accounts billable, accounts payable, and financial reporting to stakeholders
- Work with the HIE Director to manage all financial and administrative matters

Organizational Chart
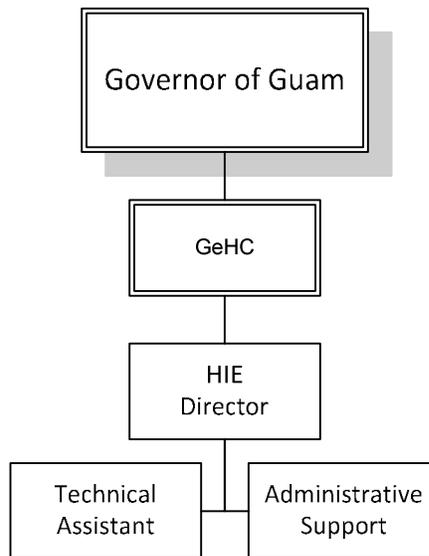
9.0   Project Budget

The document below represents the budget for the project through the end on the Cooperative Agreement Program.

10/1/12 - 9/30/13	Budget
REVENUE	
Federal Grant	$ 456,659
Guam Stakeholders	$ -
Total	$ 456,659
EXPENSE	
Salaries	$ 74,308
Fringe	$ 25,163
Travel	$ 39,744
Equipment	$ 6,484
Supplies	$ 3,600
Infrastructure	$ 125,000
Consulting Assistance	$ 182,360
Total	$ 456,659
10/1/13 - 3/15/14	Budget
REVENUE	
Federal Grant	$ 204,337
Guam Stakeholders	$ -
Total	$ 204,337
EXPENSE	
Salaries	$ 42,755
Fringe	$ 16,984
Travel	$ 10,798
Equipment	$ -
Supplies	$ 1,800
Infrastructure	$ 125,000
Consulting Assistance	$ 7,000
Total	$ 204,337

10.0 Risk Management and Mitigation Strategies

Risk mitigation involves the identification of risk and the development of strategies to manage and reduce or eliminate it. Risk management is the systematic process of identifying, analyzing, and responding to identified risks. It includes maximizing the probability and consequences of positive events, and minimizing the probability and consequences of adverse events to project objectives.

10.1 RISK MANAGEMENT PLAN

Identified Risk	Mitigation Plan
1. Late project approval from ONC	A. Request approval within timelines agreed to in the project plan
2. Set achievable expectations	A. Build solution using proven technology
	B. Use a pilot to demonstrate the functionality
	C. Review expectations with stakeholders including ONC
	D. Review technological capabilities of providers
3. GeHC fails to monitor project progress	A. Use sub-committee structure for faster response
	B. Use project management process to track and measure progress
4. Operating costs are unsustainable	A. Use the selection process to negotiate sustainable rates
	B. Ensure new solution has rates for HIE within budget capacity
	C. Revise the financial sustainability plan
	D. Seek additional funding sources or raise fees
5. Medicaid fails to complete SMHP and I-APD on time	A. Escalate issues to Governors office
	B. Schedule stakeholder meetings to gain support
	C. Escalate to HHS for support
6. RFP process is delayed	A. Compress the timeline
	B. Conduct project meetings with DOA
	C. Appeal to the ONC for support and information
7. Time delays on project deliverables	A. Use project management process to track and measure progress
	B. Pressure the solution partner for additional resources to accelerate implementation
	C. Appeal to the ONC for additional authority and support
8. Inability of stakeholders to contribute to costs	A. Provide stakeholder education on an ROI for them
	B. Seek alternative and less expensive technology
9. Failure of Medicaid to share equitability in the cost of the HIE	A. Meet with Medicaid decision makers to review interactions, use-cases and gain Medicare support
	B. Appeal to CMS for direct support

11.0 Project Plan Timeline

January 2013 Work Activity

	Start	End	Duration	Responsibility	Deliverables	Guam BIT Expenditure	Hielix/Willow Expenditure
Approve Project Plan	1/1/2013	1/31/2013	31 days	GeHC	Process defined		
Determine Procurement Process	1/7/2013	1/31/2013	24 days	Guam BIT	Due diligence process		
Determine Vendor Selection Process	1/21/2013	1/31/2013	10 days	Consultant Service	Decision criteria established		
Determine Key Decision Criteria	1/21/2013	1/31/2013	10 days	Consultant Service	RFP Framework established		
Develop RFP Framework	1/21/2013	1/31/2013	10 days	Consultant Service	Vendor list established		
Identify RFP Vendor List	1/21/2013	1/31/2013	10 days	Consultant Service	State partners identified		
Determine Potential State Partners	1/21/2013	1/31/2013	10 days	Consultant Service	Selection criteria established		
Develop State Partner Selection Criteria	1/21/2013	1/31/2013	10 days	Consultant Service	Assistance requirements identified		
Medicaid SMHP/IAPD Assistance	1/21/2013	1/31/2013	10 days	Consultant Service	Assistance requirements identified		
VA/DoD Pilot Program Assistance	1/21/2013	1/31/2013	10 days	Consultant Service	Communications plan complete		
Stakeholder Communications Plan	1/21/2013	1/31/2013	10 days	Consultant Service	Meetings established		
Establish Initial State Contacts	1/28/2013	1/31/2013	4 days	Consultant Service	Meetings established		
Establish Initial Vendor Contacts	1/28/2013	1/31/2013	4 days	Consultant Service			
January 2013 Total							$17,500

February 2013 Work Activity

	Start	End	Duration	Responsibility	Deliverables	Guam BIT Expenditure	Hielix/Willow Expenditure
Meet with Alaska	2/1/2013	2/28/2013	28 days	Team	Meetings conducted		
Meet with Oregon	2/1/2013	2/28/2013	28 days	Team	Meetings conducted		
Meet with Delaware	2/1/2013	2/28/2013	28 days	Team	Meetings conducted		
Meet with CHIC - MN HIE	2/1/2013	2/28/2013	28 days	Team	Meetings conducted		
Meet with Hawaii	2/1/2013	2/28/2013	28 days	Team	Meetings conducted		
Complete an RFP for Vendors	2/1/2013	2/28/2013	28 days	Consultant Service	RFP is completed - ready for distribution		
Medicaid SMHP/IAPD Assistance	2/1/2013	2/28/2013	28 days	Consultant Service	Provide assistance as required		
VA/DoD Pilot Program Assistance	2/1/2013	2/28/2013	28 days	Consultant Service	Provide assistance as required		
Review List of Potential Vendors for RFP	2/25/2013	2/28/2013	3 days	Team	Vendors selected		
Stakeholder Communications	2/25/2013	2/28/2013	3 days	Guam BIT	Project update to stakeholders		
February 2013 Total							$21,000

March 2013 Work Activity

	Start	End	Duration	Responsibility	Deliverables	Guam BIT Expenditure	Hielix/Willow Expenditure
Select Partner State	3/1/2013	3/8/2013	8 days	GeHC	Partner identified and selected		
Medicaid SMHP/IAPD Assistance	3/1/2013	3/31/2013	31 days	Consultant Service	Provide assistance as required		
Publish RFP	3/1/2013	3/31/2013	31 days	Guam BIT	Process commenced		
VA/DoD Pilot Program Assistance	3/1/2013	3/31/2013	31 days	Consultant Service	Provide assistance as required		
Begin Negotiations with Partner State	3/11/2013	3/31/2013	20 days	Consultant Service	Contract document prepared		
Stakeholder Communications	3/25/2013	3/31/2013	6 days	Guam BIT	Project update to stakeholders		
March 2013 Total							$17,500

April 2013 Work Activity

Medicaid SMHP/IAPD Assistance	4/1/2013	4/30/2013	30 days	Consultant Servic	Provide assistance as required
VA/DoD Pilot Program Assistance	4/1/2013	4/30/2013	30 days	Consultant Servic	Provide assistance as required
Continue Negotiations with Partner State	4/1/2013	4/15/2013	30 days	Team	Contract negotiaitons in process
Tech-Receive Responses from RFP	4/1/2013	4/1/2013	1 day	Guam BIT	RFP Responses received
Tech-Evaluate RFP Responses	4/2/2013	4/19/2013	17 days	Consultant Servic	RFP resposnes evaluated
Tech-Select Vendor for Negotiations	4/22/2013	4/30/2013	8 days	GeHC	Vendor selected
Begin the Development Migration Strateg	4/22/2013	4/30/2013	8 days	Consultant Servic	Migration plan initiated
Stakeholder Communications	4/25/2013	2/28/2013	4 days	Guam BIT	Project update to stakeholders
April 2013 Total					$17,500

May 2013 Work Activity

Medicaid SMHP/IAPD Assistance	5/1/2013	5/31/2013	31 days	Consultant Servic	Provide assistance as required
VA/DoD Pilot Program Assistance	5/1/2013	5/31/2013	31 days	Consultant Servic	Provide assistance as required
Continue Negotiations with Partner State	5/1/2013	5/31/2013	31 days	Team	Contract negotiaitons in process
Tech-Begin Negoiations with Selected Ve	5/1/2013	5/31/2013	31 days	Team	Contract negotiaitons in process
Continue Developing Migration Strategy	5/1/2013	5/31/2013	31 days	Consultant Servic	Migration plan in process
Stakeholder Communications	5/28/2013	5/31/2013	5 days	Guam BIT	Project update to stakeholders
May 2013 Total					$17,500

June 2013 Work Activity

VA/DoD Pilot Program Assistance	6/1/2013	6/30/2013	30 days	Consultant Servic	Provide assistance as required
Medicaid SMHP/IAPD Assistance	6/1/2013	6/30/2013	30 days	Consultant Servic	Provide assistance as required
Complete Negotiations with Partner State	6/1/2013	6/14/2013	14 days	Team	Contract documents approved
Tech-Complete Negoiations with Selecte	6/1/2013	6/14/2013	14 days	Team	Vendor partner selected
Conduct Comparative Analysis	6/17/2013	6/21/2013	5 days	Consultant Servic	Analysis completed
Prepare Recommendations for GeHC	6/24/2013	6/26/2013	3 days	Consultant Servic	Recommendation finalized
Approve Preferred Vendor or State Optio	6/27/2013	6/28/2013	2 days	GeHC	Preferred option approved
Finalize Migration Strategy	6/1/2013	6/28/2013	28 days	Consultant Servic	Migration strategy complete
Stakeholder Communications	6/24/2013	6/28/2013	4 days	Guam BIT	Project update to stakeholders
June 2013 Total				$ 125,000	$ 21,000

July 2013 Work Activity

VA/DoD Pilot Program Assistance	7/1/2013	7/31/2013	31 days	Consultant Servic	VA/DoD connection complete
Medicaid SMHP/IAPD Assistance	7/1/2013	7/31/2013	31 days	Hielix/Willow	SMHP/I-APD Completed
Begin Infrastructure Implementation	7/1/2013	7/31/2013	31 days	Guam BIT	Solution implementation starts
Project Monitoring and Oversight	7/1/2013	7/31/2013	31 days	Hielix/Willow	Monitoring in process
Stakeholder Communications	7/29/1931	7/31/2013	3 days	Guam BIT	Project update to stakeholders
July 2013 Total					$17,500

Activity	Start Date	End Date	Duration	Vendor	Milestone	Cost
Continue Infrastructure Implementation	8/1/2013	8/30/2013	30 days	Guam BIT	Solution implementation in process	
Project Monitoring and Oversight	8/1/2013	8/30/2013	30 days	Consultant Service	Project monitoring in process	
Stakeholder Communications	8/25/2013	8/30/2013	5 days	Guam BIT	Project update to stakeholders	
August 2013 Total						$14,000
September 2013 Work Activity						
Continue Infrastructure Implementation	9/1/2013	9/30/2013	30 days	Guam BIT	Solution implementation in process	
Project Monitoring and Oversight	9/1/2013	9/30/2013	30 days	Consultant Service	Project monitoring in process	
Stakeholder Communications	9/26/2013	9/30/2013	3 days	Guam BIT	Project update to stakeholders	
September 2013 Total						$10,500
October 2013 Work Activity						
Finalize Infrastructure Implementation	10/1/2013	10/31/2013	31 days	Guam BIT	Solution implementationin complete	
Project Monitoring and Oversight	10/1/2013	10/31/2013	31 days	Consultant Service	Project monitoring in process	
Stakeholder Communications	10/28/2013	10/31/2013	3 days	Guam BIT	Project update to stakeholders	
October 2013 Total						$7,000
November 2013 Work Activity						
Complete Infrastructure Testing	11/1/2013	11/30/2013	30 days	Guam BIT	Project testing complete	
Stakeholder Communications	7/29/1931	11/30/2013	3 days	Guam BIT	Project update to stakeholders	
November 2013 Total						
December 2013 Work Activity						
HIE Infrastructure Operational - final paymen	12/1/2013	12/13/2013	13 days	Guam BIT	Solution fully operational	
Stakeholder Communications	12/16/2013	12/20/2013	5 days	Guam BIT	Project Update to Stakeholders	
December 2013 Total						$125,000
January 2014 Work Activity						
HIE Infrastructure Operational	1/1/2014	1/31/2014	31 days	Guam BIT	Solution fully operational	
Stakeholder Communications	1/27/2014	7/31/2013	3 days	Guam BIT	Project Update to Stakeholders	
January 2014 Total						
Sub-Total - Guam BIT Vendor						$ 250,000
Sub-Total - Hielix/Willow						$161,000
Travel						$ 25,000
						$ 436,000

APPENDIX A—GeHC Organizational Structure and Membership List

The Guam eHealth Collaborative (GeHC)

James Gillan - Department of Public Health & Social Services

Vince Quichocho - Guam Memorial Hospital

Joe Grecia - Department of Mental Health & Substance Abuse

Ed Cruz - Bureau of Information Technology

Paula Blas - Guam Retirement Fund

Dr. Taitano - Guam Medical Society

Carla Haddock - Guam Nursing Association

Karen Song - Guam Pharmacists Association

Senator Dennis Rodriguez - Guam Legislature

Benita Manglona - Department of Administration

John Rios - Bureau of Budget and Management Research

Mike Tsai - TakeCare Insurance

Frank Campillo – Chamber of Commerce

Albert Gurasamy - Home Care and Hospice

APPENDIX B --Policies and Procedures to Protect Privacy and Security of Health Information

Subject: **1. Privacy and Confidentiality**	
Subsection: **1.1 PHI Protection**	Effective Date:
Author:	Original Date:
Review by:	Revision Date:
Approval by:	Document Reference

I. Purpose
To ensure that the identity and location of protected health information (PHI) are protected at all times.

II. Policy
Guam Health Information Exchange (GeHC) shall establish policies and procedures to ensure that the identity and location of PHI are protected at all times and avoid any unauthorized disclosure of patient information. Furthermore, it is the intent of this policy that encryption, user authentication, message integrity, and support for non-repudiation will comply with all related legislation.

III. Procedure:
PHI will be protected throughout all modules within the HIE system/Guam HIE Web Portal, including but not limited to the Direct Secure Messaging Service, Record Locator Service (RLS) Query, Security Manager, and Consent Manager.

In addition to agreements and provider policies protecting unauthorized access to or disclosure of PHI, GeHC requires it's HIE software vendor to implement appropriate and necessary technologies that meet or exceed the minimum requirements (http://www.healthit.gov/policy-researchers-implementers/privacy-security-policy) for health information privacy and security. These should include, but are not limited to:

1. Digital Certificates: Issued one per user per system (computer) profile, with no sharing of Digital Certificates allowed. Initially a Guam-based central certificate authority (CA).
2. Encryption/ secure transmission of information
3. User Authentication for each action (The 2-factor authentication is required for users of all modules -RLS query, Security Manager and Consent Manager).
4. Hidden name or assigned number in audit list queries
5. Role-based access/Access Control

IV. Definitions:

V. References/Related Policies:
HIPAA Security Rule, 45 C.F.R. § 164.304 and 312 (a)(2)(iv), (e)(2)(ii): http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&SID=a22b7267332f605932cf321dcf29584c&rgn=div8&view=text&node=45:1.0.1.3.79.3.27.2

&idno=45; http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&SID=a22b7267332f605932cf321dcf29584c&rgn=div8&view=text&node=45:1.0.1.3.79.3.27.6&idno=45

HITECH § 13402(h):

http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html

The Electronic Healthcare Network Accreditation Commission (EHNAC) - Section 1: Privacy and Confidentiality – Measures to Ensure Data Privacy and Confidentiality.

Subject: **1. Privacy and Confidentiality**	
Subsection: **1.2 Disclosure Safeguards**	Effective Date:
Author:	Original Date:
Review by:	Revision Date:
Approval by:	Document Reference: Business Associate Agreement

I. Purpose
To ensure that the identity and location of protected health information (PHI) are protected at all times.

II. Policy
Provider Organizations (POs) shall use appropriate safeguards to prevent use or disclosure of PHI otherwise than as permitted by signed Business Associate Agreements (BAAs), including appropriate administrative, physical, and technical safeguards that protect the confidentiality, integrity, and availability of that PHI.

III. Procedure:
PHI will be protected throughout all modules within the Health Information Exchange (HIE) system/Guam HIE Web Portal, including but not limited to the Direct Secure Messaging Service, Record Locator Service (RLS) Query, Security Manager, and Consent Manager.

Appropriate safeguards shall be those identified in the HIPAA Security Rule as "required" and, to the extent that implementation is reasonable, those that are identified as "addressable." Each PO shall have appropriate written privacy and security policies in place by their respective effective date of initial participation in HIE.

IV. Definitions:

V. References/Related Policies:
Business Associate/Covered Entity Sample Agreement:
http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html

The Electronic Healthcare Network Accreditation Commission (EHNAC) - Section 1: Privacy and Confidentiality – Measures to Ensure Data Privacy and Confidentiality.

Subject: **1. Privacy and Confidentiality**	
Subsection: **1.3 Role-based Access**	Effective Date:
Author:	Original Date:
Review by:	Revision Date:
Approval by:	Document Reference:

I. Purpose
To ensure that the identity and location of protected health information (PHI) are protected at all times,

II. Policy
The purpose of this policy is to ensure that role-based access is implemented and effective to limit users of the GeHC to access PHI for which they are granted access.

III. Procedure:
All users are assigned one or more roles/privileges for accessing information and only those with the appropriate authorization may access PHI. The access roles currently available for users are:

1. Patient Query and Discovery (used by most authorized users)
2. Audit Log Query and Reporting (used by authorized privacy officers)
3. Consent Management (used by authorized personnel to manage opt out requests received from POs).

IV. Definitions:

V. References/Related Policies:
HITECH §13405(b)(1)(A):
 http://www.hipaasurvivalguide.com/hitech-act-13405.php

45 Code of Federal Regulations (C.F.R.) §164.502(b):
http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&SID=ee367bb6d87ae03bcbd87437bff876b9&rgn=div8&view=text&node=45:1.0.1.3.79.5.27.3&idno=45

The Electronic Healthcare Network Accreditation Commission (EHNAC) - Section 1: Privacy and Confidentiality – Measures to Ensure Data Privacy and Confidentiality.

Subject: **1. Privacy and Confidentiality**	
Subsection: **1.4 Prohibitions of Data Use**	Effective Date:
Author:	Original Date:
Review by:	Revision Date:
Approval by:	Document Reference:

I. Purpose
To ensure that the identity and location of protected health information (PHI) are protected at all times.

II. Policy
The GeHC will not sell or otherwise use PHI in such a way as to violate privacy or confidentiality of any healthcare data and/or information.

III. Procedure:

IV. Definitions:

V. References/Related Policies:
http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html
The Electronic Healthcare Network Accreditation Commission (EHNAC) - Section 1: Privacy and Confidentiality – Measures to Ensure Data Privacy and Confidentiality.

Subject: **1. Privacy and Confidentiality**	
Subsection: **1.5 Virus Security**	Effective Date:
Author:	Original Date:
Review by:	Revision Date:
Approval by:	Document Reference:

I. Purpose
To ensure that the identity and location of protected health information (PHI) are protected at all times.

II. Policy
POs in the GeHC will ensure security controls that meet applicable industry or federal standards so that the information and data transmitted and any method of transmitting such information will not introduce any viruses, worms, and unauthorized cookies, Trojans, malicious software or "malware".

III. Procedure:
These controls will prohibit any other program, routine, subroutine, or data designed to disrupt the proper operation of a System or any part thereof or any hardware (including mobile devices) or software used by a PO in connection therewith, or which, upon the occurrence of a certain event, the passage of time, or the taking of or failure to take any action will cause a system or any part thereof or any hardware (including laptop computers), software or data used by a PO in connection therewith, to be improperly accessed, destroyed, damaged, or otherwise made inoperable.

In the absence of applicable industry standards, each PO will defer to the ISO 9001 standard to ensure compliance with this section. Inappropriate use of computer workstations can expose a PO to risks such as viruses, compromise of information systems, and breeches of confidentiality. Basic security measures for workstation security include privacy screens, screen savers with password options, timed log-outs.

IV. Definitions:

V. References/Related Policies:
45 C.F.R. § 164.308(a)(5)(ii)(B):
http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&SID=363fae49282e64e5536ba583e530624f&rgn=div8&view=text&node=45:1.0.1.3.79.3.27.4&idno=45

The Electronic Healthcare Network Accreditation Commission (EHNAC) - Section 1: Privacy and Confidentiality – Measures to Ensure Data Privacy and Confidentiality.

Subject: **1. Privacy and Confidentiality**	
Subsection: **1.6 User Roles**	Effective Date:
Author:	Original Date:
Review by:	Revision Date:
Approval by:	Document Reference:

I. Purpose
To ensure that the identity and location of protected health information (PHI) are protected at all times.

II. Policy
GeHC shall will maintain a list of all individuals, contractors, and BAs with access to e-PHI and their assigned user roles and job title.

III. Procedure:
This listing of users with access to e-PHI will be regularly updated by the Privacy Officer to ensure accuracy and verified at least annually.

IV. Definitions:

V. References/Related Policies:
The Electronic Healthcare Network Accreditation Commission (EHNAC) - Section 1: Privacy and Confidentiality – Measures to Ensure Data Privacy and Confidentiality.

Subject: **1. Privacy and Confidentiality**	
Subsection: **1.7 Portable Devices**	Effective Date:
Author:	Original Date:
Review by:	Revision Date:
Approval by:	Document Reference:

I. Purpose
To ensure that the identity and location of protected health information (PHI) are protected at all times.

II. Policy
Each PO will have policies and procedures to enforce security measures to prohibit storage of e-PHI on portable devices. Each POs, and all relevant subcontractors and developers will protect PHI.

III. Procedure:
All users or those with access to PHI through the GeHC are prohibited from storing such information, unencrypted, on any portable device; this includes, but is not limited to laptop computers and cellular phones.

IV. Definitions:

V. References/Related Policies:

45 CFR §§ 164.530(c): http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&SID=a22b7267332f605932cf321dcf29584c&rgn=div8&view=text&node=45:1.0.1.3.79.5.27.15&idno=45

The Electronic Healthcare Network Accreditation Commission (EHNAC) - Section 1: Privacy and Confidentiality – Measures to Ensure Data Privacy and Confidentiality.

Subject: **1. Privacy and Confidentiality**	
Subsection: **1.8 Wireless Security**	Effective Date:
Author:	Original Date:
Review by:	Revision Date:
Approval by:	Document Reference:

I. Purpose

To ensure that the identity and location of protected health information (PHI) are protected at all times.

II. Policy

The GeHC ensures appropriate security is in place for wireless networks to protect the privacy of data during transmission and in storage.

III. Procedure:

The Guam HIE Privacy and Security Office is responsible for developing and maintaining standards, providing implementation guidelines, and providing security training. They are also responsible for monitoring network security and enforcing the implementation of security policies, standards, and enterprise-wide procedures accordingly. No devices shall be connected to a wireless network unless they have a valid service set identifier (SSID).

IV. Definitions:

V. References/Related Policies:
http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/remoteuse.pdf

The Electronic Healthcare Network Accreditation Commission (EHNAC) - Section 1: Privacy and Confidentiality – Measures to Ensure Data Privacy and Confidentiality.

Subject: **1. Privacy and Confidentiality**	
Subsection: **1.9 Patch Management**	Effective Date:
Author:	Original Date:
Review by:	Revision Date:
Approval by:	Document Reference:

I. Purpose
To ensure that the identity and location of protected health information (PHI) are protected at all times.

II. Policy
The GeHC maintains configuration standards that include patch management for systems that store, transmit, or access e-PHI, including workstations.

III Procedure:
In the event of security vulnerability, a process will be followed to evaluate the criticality and applicability of the patch. A risk assessment will be performed on all servers on the network. This assessment will include the criticality of the data on the server, the impact of server downtime on enterprise operations and the vulnerability of the server to internal and external attack.

IV. Definitions:

V. References/Related Policies:
http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/nist800111.pdf

The Electronic Healthcare Network Accreditation Commission (EHNAC) - Section 1: Privacy and Confidentiality – Measures to Ensure Data Privacy and Confidentiality.

Subject: **1. Privacy and Confidentiality**	
Subsection: **1.10 Encryption Protocol**	Effective Date:
Author:	Original Date:
Review by:	Revision Date:
Approval by:	Document Reference:

I. Purpose
To ensure that the identity and location of protected health information (PHI) are protected at all times.

II. Policy
It is the intent of this policy that transmitted e-PHI is encrypted and not improperly modified without detection.

III. Procedure:
E-PHI will have field level encryption and integrity controls. Therefore, data that does not decrypt with the proper encryption will be reviewed through runtime statistics and audit log to verify when and how the file was processed for field encryption.

IV. Definitions:

V. References/Related Policies:
45 C.F.R. § 164.312(e)(2)(i): http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&SID=ec7dc51ee84d7b47273a28b648581fff&rgn=div8&view=text&node=45:1.0.1.3.79.3.27.6&idno=45

The Electronic Healthcare Network Accreditation Commission (EHNAC) - Section 1: Privacy and Confidentiality – Measures to Ensure Data Privacy and Confidentiality.

Subject: **1. Privacy and Confidentiality**	
Subsection: **1.11 Business Associates**	Effective Date:
Author:	Original Date:
Review by:	Revision Date:
Approval by:	Document Reference: Business Associate Agreement See Guam Participation Agreement

I. Purpose
To ensure that the identity and location of protected health information (PHI) are protected at all times.

II. Policy
The data exchanged through the GeHC contains PHI. Furthermore, some, but not all, POs are either Covered Entities or Business Associates (BA) of Covered Entities, (as defined in the HIPAA Regulations). POs are limited to exchanging data through the Guam HIE for only Permitted Purposes (as defined in HIPAA) and the POs do not intend to become BAs of each other by signed agreement.

III. Procedure:
The Guam Participation Agreement is not intended to serve as a Business Associate Agreement (BAA) among the POs. To support the privacy, confidentiality and security of 'the Data' (as defined in the Agreement) and the GeHC, will require the parties to agree as follows:

1. If the PO is a Covered Entity, the PO does, and at all times shall, comply with HIPAA to the extent applicable.
2. If the PO is a BA of a Covered Entity, PO does, and shall at all times, comply with the provisions of its BAA and Applicable Law.
3. GeHC shall be deemed a BA of each PO and will enter into a BAA as provided by each PO reasonably acceptable to GeHC.

IV. Definitions:

V. References/Related Policies:
Business Associate/Covered Entity Sample Agreement:
http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html

The Electronic Healthcare Network Accreditation Commission (EHNAC) - Section 1: Privacy and Confidentiality – Measures to Ensure Data Privacy and Confidentiality.

Subject: **2. Technical Performance**	
Subsection: **2.1 Transmission of Data**	Effective Date:
Author:	Original Date:
Review by:	Revision Date:
Approval by:	Document Reference: Trading Partner Agreement

I. Purpose
The GeHC will comply with all applicable federal and state requirements and regulations in regards to Trading Partners.

II. Policy
The GeHC will ensure that all eligible electronic transactions are received and timely submitted with identified GeHC trading partners who accept or generate transactions electronically.

III. Procedure:
In order to ensure interoperability between the GeHC and its trading partners, the GeHC will dictate standards to exchange clinical data (such as data formats) for providers and stakeholders to conform to. The GeHC will make available real-time transactions, in accordance with agreements with its trading partners.

The GeHC will have an acknowledgment system and a trading partner tracking system that documents response times and procedures that are appropriate to different levels of requests. This system will be developed and monitored by the Privacy Officer or designee.

GeHC will acknowledge partner inquires within three hours and will respond with a plan of action to open inquiries prior to the conclusion of the next business day. Critical (as flagged) inquiries will receive a response within four hours within normal business hours.   The GeHC will follow escalation procedures to follow the inquiry to completion coordinated through the Privacy Officer.

The GeHC performs annual applications and data criticality analysis by assessing the relative criticality of specific applications and data in support of other plan components and maximum technical performance.

IV. Definitions:

V. References/Related Policies:
45 C.F.R. § 164.308(a)(7)(ii)(E)
Trading Partner Agreement
The Electronic Healthcare Network Accreditation Commission (EHNAC) - Section 2: Technical Performance.

Subject: **2. Technical Performance**	
Subsection: **2.2 Data Validation**	Effective Date:
Author:	Original Date:
Review by:	Revision Date:
Approval by:	Document Reference:

I. Purpose

The GeHC will comply with all applicable federal and state requirements and regulations in regards to Trading Partners.

II. Policy

GeHC will ensure successful delivery of transactions to Trading Partners.

III. Procedure:

The GeHC HIE infrastructure will ensure that 100% of transactions are either delivered successfully to the trading partner or are reported to the originator as undeliverable (thorough automatic message). The GeHC, through the responsibilities of the Privacy Officer, will also provide for the monitoring and reporting of failed data transmissions to the sender. Reporting shall specifically indicate the source of the problem (if known). The Privacy Officer will complete a weekly reconciliation of all error messages and problems for auditing and further system development.

IV. Definitions:

V. References/Related Policies:

The Electronic Healthcare Network Accreditation Commission (EHNAC) - Section 2: Technical Performance.

Subject: **2. Technical Performance**	
Subsection: **2.3 System Availability**	Effective Date:
Author:	Original Date:
Review by:	Revision Date:
Approval by:	Document Reference:

I. Purpose

The GeHC will comply with all applicable federal and state requirements and regulations in regards to Trading Partners.

II. Policy

The GeHC HIE will maintain minimum system availability for Trading Partner access.

III. Procedure:

The GeHC HIE infrastructure will have a minimum system availability (and scheduled redundancy) that assures system access for 98.0% of contracted hours. This requirement shall not include outages due to unforeseen events, (listed as acts of God per contract language/Business Associate Agreement).

The GeHC HIE infrastructure will notify trading partners regarding critical service outages outside the standard maintenance schedule prior to the planned outages. The GeHC will also develop a Disaster Response Plan that will be updated annually by the Privacy Officer.

IV. Definitions:

V. References/Related Policies:

The Electronic Healthcare Network Accreditation Commission (EHNAC) - Section 2: Technical Performance.

Subject: **2. Technical Performance**	
Subsection: **2.4 Industry Standards**	Effective Date:
Author:	Original Date:
Review by:	Revision Date:
Approval by:	Document Reference:

I. Purpose
The GeHC will comply with all applicable federal and state requirements and regulations in regards to Trading Partners.

II. Policy
The GeHC will support generally accepted industry standard formats and those required by federal and state regulations as detailed in Trading Partner Agreements.

III. Procedure:
The GeHC will have an established implementation plan for compliance with all applicable federal and state adopted rules and implementation guides. This plan will include a sequence and timetable for implementation within mandatory timeframes.

The GeHC will maintain a current analysis of any federal or state privacy or security laws that the GeHC reasonably believes apply to information stored or transmitted by the GeHC (e.g., security breach notification laws). The GeHC will comply with any such laws.

IV. Definitions:

V. References/Related Policies:
The Electronic Healthcare Network Accreditation Commission (EHNAC) - Section 2: Technical Performance.

Subject: **2. Technical Performance**	
Subsection: **2.5 Capacity Monitoring**	Effective Date:
Author:	Original Date:
Review by:	Revision Date:
Approval by:	Document Reference: Service Level Agreement

I. Purpose

The GeHC will comply with all applicable federal and state requirements and regulations in regards to Trading Partners.

II. Policy

The GeHC will ensure needed system capacity plan for optimal performance.

III. Procedure:

The GeHC will have the ability to measure system capacity and have developed an on-going monitoring capability for that system capacity. The GeHC will have a formal system capacity plan for handling peak load and expansion including a demonstration of 99.5% availability on communication exchange components per the advertised service level agreements. This requirement does not include unforeseen outages (Referred to as acts of God in contract).

The GeHC will establish and implement disaster recovery procedures as part of their risk management plan that will restore any loss of data, with the Recovery Point Objective not to exceed 48 hours and the Recovery Time Objective not to exceed 48 hours for critical transaction processing.

IV. Definitions:

V. References/Related Policies:

The Electronic Healthcare Network Accreditation Commission (EHNAC) - Section 2: Technical Performance.

Subject: **2. Technical Performance**	
Subsection: **2.6 Auditing**	Effective Date:
Author:	Original Date:
Review by:	Revision Date:
Approval by:	Document Reference:

I. Purpose
The GeHC will comply with all applicable federal and state requirements and regulations in regards to Trading Partners.

II. Policy
The GeHC will provide a clear and accurate audit trail of all data transactions for a minimum of seven years.

III. Procedure:
Audit Trails record user names, transaction, information source, status, and time of each transaction, as well as transaction dependent information such as patient name for relevant queries.

The GeHC requires their POs to perform quarterly audits on authorized user accounts and compare the information accessed to the care that was provided by the authorized user. Consumers must be notified immediately when an authorized user has inappropriately accessed their information.
IV. Definitions:

V. References/Related Policies:
The Electronic Healthcare Network Accreditation Commission (EHNAC) - Section 2: Technical Performance.

Subject: **2. Technical Performance**	
Subsection: **2.7 Storage and Retrieval**	Effective Date:
Author:	Original Date:
Review by:	Revision Date:
Approval by:	Document Reference:

I. Purpose

The GeHC will comply with all applicable federal and state requirements and regulations in regards to Trading Partners.

II. Policy

The GeHC will have sufficient archive, storage and retrieval capacity for transactions.

III. Procedure:

The GeHC will have an off-site minimum of six-month back-up archive, storage and retrieval capability for all transactions and adhere to all applicable federal and state regulations. The GeHC will have one-day storage and retrieval capability for real-time transactions.

Data Center Description

Data Center	
Address	<Include>
Site Type	Switch/Node/Collocation Facility (Major)
Equipment	DMS switch, Transport Equipment, CLR
Status	On Net, Dual Entrance
Power Protection	Battery Back-up; 1000 KW CAT generator
Video Monitoring	Yes
Fire Suppression	Dry pipe pre-action
Access	XO key card

IV. Definitions:

V. References/Related Policies:

The Electronic Healthcare Network Accreditation Commission (EHNAC) - Section 2: Technical Performance.

Subject: **2. Technical Performance**	
Subsection: **2.8 Internet**	Effective Date:
Author:	Original Date:
Review by:	Revision Date:
Approval by:	Document Reference:

I. Purpose
The GeHC will comply with all applicable federal and state requirements and regulations in regards to Trading Partners.

II. Policy
The GeHC will maintain security on its websites and provide capacity and bandwidth adequate for business needs.

III. Procedure:
The GeHC will ensure that internal databases cannot be modified directly through an external web site, unless made securely, by authenticated users and contain integrity checks. Otherwise, all modifications to databases are to be made first only to external databases (e.g. those kept on the web server) and integrity checks are to be made on the external database prior to synchronization with any internal database.

The GeHC will authenticate the PO sending or receiving healthcare data (Includes as unique user, PO and/or HISP). The GeHC will have a process in place to monitor Internet bandwidth and communication server performance daily.

The GeHC will respond to a successful intrusion or attack from the Internet within 2 hours of alarm generation or notification. The Privacy Officer or designee will check public security web sites, Web O/S vendor and web application vendors on at least a weekly basis to identify potential security weaknesses and update web server O/S and application configurations to eliminate or reduce those known weaknesses. The GeHC will monitor and/or block intrusion attempts or attacks from the Internet and provide alarms to appropriate personnel.

The GeHC will have documented web server security configurations to protect the web server from attack or intrusion. The Privacy Officer will ensure that any file transfer servers are not configured to reside on a firewall in such a manner that the file transfer server may be able to be accessed through a port-forwarding configuration through the firewall.

The following deployed exchange security measures to prevent and detect security threats and intrusions are shown below:

Intrusion detection	At the firewall level (Basic)
Vulnerability assessments	Will be supported Quarterly

Data encryption	Both symmetric and asymmetric encryption are supported: • Symmetric Key Based: Advanced Encryption Standard (AES) • Asymmetric key Based (public key cryptography): RSA
Authentication, authorization, access controls, audit and compliance functions	• PKI based two-way SSL node authentication • Role-based access control (RBAC) supported • Every transactions (auditable events) are logged for future audit review • Compliant with federal requirements for security:– Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology; Final Rule”

IV. Definitions:

V. References/Related Policies:

The Electronic Healthcare Network Accreditation Commission (EHNAC) - Section 2: Technical Performance.

Subject: **3. Business Practices**	
Subsection: **3.1 Trading Partner Agreements**	Effective Date:
Author:	Original Date:
Review by:	Revision Date:
Approval by:	Document Reference:

I. Purpose
GeHC will follow accepted business practices.

II. Policy
It is the expressed policy of GeHC to require compliance audits (annual and random) to monitor the use of the HIE and to ensure compliance.

III. Procedure:
The GeHC will meet or exceed the service levels as described in the data sharing agreements between trading partners. Furthermore, the GeHC will ensure that any trading partner agreements do not endanger related compliance with the Electronic Healthcare Network Accreditation Commission (EHNAC) HIE Accreditation Criteria.

The GeHC will require compliance announced audits (annual and random) to monitor the use of the HIE and to ensure compliance with applicable federal and state/territory privacy law and HIE policies, and to include the following in the audit:

1. Verification that consents are on file (and available for inspection) at the appropriate entity (HIE or trading partner) for patients whose PHI is accessed via the HIE; and
2. Each HIE BAA requires that authorized users who access PHI do so for authorized purposes.

The GeHC will conduct (annual and random) compliance audits, and if necessary, more frequently if a HIE participant has deficiencies in any previous compliance audit.   All compliance audits will ensure each PO is in compliance with the privacy terms of their BAA. If deficiencies are noted and appropriate corrective actions have not improved the situation within 7 business days , the GeHC reserves the right to suspend access of the PO or specific user(s). Pos have the right to appeal a suspension directly to the GeHC Board.

Access suspension appeals are limited to participants who are in 'regular' positions classified by their organization (e.g. successfully completed a probationary period). Users must submit their appeals to GeHC within 15 working days of notice of the suspension.

IV. Definitions:

V. References/Related Policies:
The Electronic Healthcare Network Accreditation Commission (EHNAC) - Section 3: Business Practices.

Subject: **3. Business Practices**	
Subsection: **3.2 User Access**	Effective Date:
Author:	Original Date:
Review by:	Revision Date:
Approval by:	Document Reference:

I. Purpose
GeHC will follow accepted business practices.

II. Policy
Each GeHC member can interconnect to other HIEs via accepted formats and protocols.

III. Procedure:
Each GeHC member is capable of interconnecting to other HIEs via accepted message formats and transport protocols. This will include a security mechanism to connect to a mail server, authenticate the exchange, and negotiate a security profile for subsequent message transfers.

IV. Definitions:

V. References/Related Policies:
The Electronic Healthcare Network Accreditation Commission (EHNAC) - Section 3: Business Practices.

Subject: **3. Business Practices**	
Subsection: **3.3 Consumer Engagement**	Effective Date:
Author:	Original Date:
Review by:	Revision Date:
Approval by:	Document Reference: Participation Agreement

I. Purpose
GeHC will follow accepted business practices.

II. Policy
The GeHC will assure consumer participation, access to information, and a mechanism for expressing and addressing concerns. The GeHC will encourage consumer engagement through patient / advocate representation in advisory groups, educational materials, and a feedback mechanism from consumers used for continually improving communication and services.

III. Procedure:
The GeHC will implement a comprehensive communication and education plan, in collaboration with other Territorial, State and Federal programs including the Hawaii-Pacific Regional Extension Center (REC), to educate stakeholders about the value of HIE. The GeHC will provide training and education to providers who are not currently working with the REC to ensure they are provided timely information.

The GeHC will make available periodic and on-demand reports to consumers regarding HIE system performance, compliance audit reports, and privacy violation notices.

POs will provide individuals with a simple and timely means to access their Individually Identifiable Health Information (IIHI) as mandated by the Participation Agreement.

 The Participation Agreement will require participating organizations to provide mechanisms for individuals to access their personal information for the purpose of identifying errors and resolving disputes.

IV. Definitions:

V. References/Related Policies:
The Electronic Healthcare Network Accreditation Commission (EHNAC) - Section 3: Business Practices.

Subject: **3. Business Practices**	
Subsection: **3.4 Intergovernmental Relations**	Effective Date:
Author:	Original Date:
Review by:	Revision Date:
Approval by:	Document Reference:

I. Purpose
GeHC will follow accepted business practices.

II. Policy
GeHC will develop and follow requirements as defined the Office of National Coordinator of Health Information Technology (ONCHIT). Additionally, the GeHC will assure the functionality required under the "Meaningful Use criteria, meeting the stipulated Meaningful Use schedule as defined in the American Recovery and reinvestment Act (ARRA).

III. Procedure:
The GeHC will serve as the health information service provider (HISP) for individual and unaffiliated providers who support data exchange to meet "Stage 1 Meaningful Use requirements". Coordination of payers in Guam is planned to increase e-prescribing adoption among providers.

IV. Definitions:

V. References/Related Policies:
The Electronic Healthcare Network Accreditation Commission (EHNAC) - Section 3: Business Practices.

Subject: **4. Physical Resources**	
Subsection: **4.1 Facilities**	Effective Date:
Author:	Original Date:
Review by:	Revision Date:
Approval by:	Document Reference: Risk Management Plan

I. Purpose
GeHC maintains resources that are adequate for the services provided.

II. Policy
The GeHC is responsible for maintaining the physical resources (including plant facilities and the relevant hardware and software) adequate to support the services it offers.

III. Procedure:

Access to the Facility- Workforce
The intent is to align information access with role or function in the organization. This information will be a supplement to facility control, as it will also determine each workforce member's access to certain locations in the facility.

A PO must evaluate the need for, and adequacy of controls on physical access to facilities and equipment handling PHI as part of risk management plan and Facility Security Plan. POs should document its approach to controlling physical access to facilities and equipment handling protected health information. Unauthorized physical access to the facility may be limited via door locks, electronic access control systems, security officer (for larger facilities), and video monitoring. Additionally, facilities will have major doors re-keyed, door combinations changed, and/or key cards destroyed after the termination of employees or contractors with prior access to facilities that stored e-PHI.

Access to Facility- Visitor
Access to facilities will be controlled and validated by GeHC to verify role or function including visitor control and controlled access to software programs for testing and revision. Visitors will be identified via badges and limited facility access.   Physical access controls will allow individuals with a legitimate purpose to obtain access to the facility and deny access to those without a legitimate need.

Other Facility Considerations
If a PO does not control the building they occupy or shares space with other organizations, it nonetheless remains responsible for considering and ensuring facility security. The PO can incorporate security measures into contracts with the party responsible for the building and document them in their own facility security plan.

The scope of these procedures will limit physical access to the electronic information systems and the facility in which they are housed. Basic security measures for facility security may include: locked doors, electronic access control systems, security officers (for larger facilities), and video monitoring.

The GeHC will document formal facility expansion plans in place to anticipate increased growth. The HIT Coordinator, Privacy Officer and appointed members from the POs and the GeHC Board, will review these plans at least annually.

All repairs and modifications to the physical components of a facility which are related to security such as hardware, walls, doors, and locks will be documented The use and review of the 'Facility/Hardware Maintenance and Movement Log' will be required by the Privacy Officer or designee.

When evaluating and implementing these standards, a covered entity must consider all physical access to e-PHI. This may extend outside of an actual office, and could include workforce members' homes, satellite offices, or other physical locations where they access e-PHI.

IV. Definitions:

V. References/Related Policies:
45 C.F.R. § 164.310(a)(2)(iii), (IV), and (b): http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=932f8fd8eaf00b36bb3a3e932cc69545&n=45y1.0.1.3.79.3&r=SUBPART&ty=HTML#45:1.0.1.3.79.3.27.5

45 C.F.R. § 164.308(a)(4)(ii)(A): http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=932f8fd8eaf00b36bb3a3e932cc69545&n=45y1.0.1.3.79.3&r=SUBPART&ty=HTML

The Electronic Healthcare Network Accreditation Commission (EHNAC) - Section 4: Resources

Subject: **4. Physical Resources**	
Subsection: **4.2 Personnel**	Effective Date:
Author:	Original Date:
Review by:	Revision Date:
Approval by:	Document Reference:

I. Purpose
GeHC maintains resources that are adequate for the services provided.

II. Policy
The GeHC will hire, train and retain sufficient qualified personnel to perform all tasks associated with the Guam HIE. All employees and contractors will be screened for security/background checks, prior to hire.

III. Procedure:
Training for all GeHC Board members, employees, contractors, volunteers, trainees, and others whose conduct is under the direct control of the GeHC (whether or not they are paid by the GeHC) will be conducted annually, or upon hiring a new employee with access to PHI. Evidence of the training completion will be available for inspection in the applicable training file.

The GeHC requires employee training on its privacy policies and procedures as necessary and related to their functions. Consequences and appropriate sanctions will be identified for workforce members who violate its privacy policies and procedures or the Privacy Rule.   This includes but is not limited to suspension of user access. The GeHC will define and publish an appeals process in 2013.

At a minimum, annual job training will be provided by the GeHC to include breach reporting and notification, privacy, and confidentiality, and security for all employees and contractors with access to PHI. Evidence of the training completion will be available for inspection in the applicable training file.

The GeHC maintains a current list of individuals, down to the manager level, who are responsible for HIPAA compliance including the protection of e- PHI. The information will also include BAs, contractors and their applicable title and/or job function. This listing will be available for inspection as maintained by the Privacy Officer.

IV. Definitions:

V. References/Related Policies:
45 C.F.R. § 164.308: http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=932f8fd8eaf00b36bb3a3e932cc69545&n=45y1.0.1.3.79.3&r=SUBPART&ty=HTML#45:1.0.1.3.79.3.27.4

HITECH § 13402
Territory of Guam/Hiring Policies/Employee or Subcontractor Grievances
The Electronic Healthcare Network Accreditation Commission (EHNAC) - Section 4: Resources

Subject: **5. Security**	
Subsection: **5.1 Hybrid Entities**	Effective Date:
Author:	Original Date:
Review by:	Revision Date:
Approval by:	Document Reference:

I. Purpose
GeHC will ensure proper security for PHI.

II. Policy
All communication through the Guam HIE will be fully encrypted, logged and face a firewall.

III. Procedure:
To ensure HIPAA compliance, all communication through the Guam HIE will be fully encrypted, using a Public Key Infrastructure (PKI) security model, to ensure that the identity of the client and server can be cryptographically verified.

1. Additionally, all transactions in the Guam HIE will be logged to ensure full audit capabilities. PKI security provides the encryption technologies required by electronic data interchange to meet the following security objectives:
2. Authentication - The process of proving one's identity.
3. Confidentiality - Ensuring that no one can read the message except the intended recipient.
4. Integrity - Assuring the recipient that the received message has not been altered in any way from the original.
5. Non-repudiation - A mechanism to prove that the sender/recipient actually sent/received a message.

In accordance with the Security Rule and, the GeHC will document the designated health care components of any Hybrid Entity.

Hybrid entities are required to create adequate "firewalls" between their health information and other components. Transfer of PHI held by the health care component to other components of the hybrid entity is a disclosure subject to the HIPAA privacy rule and is allowed only under the same circumstances as would make it permissible for a separate entity.

IV. Definitions:
Hybrid Entity, which is defined by HIPAA as one that uses or discloses PHI for only a part of its business operations.

V. References/Related Policies:
45 C.F.R. § 164.105: http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=932f8fd8eaf00b36bb3a3e932cc69545&n=45y1.0.1.3.79&r=PART&ty=HTML#45:1.0.1.3.79.1.27.4
The Electronic Healthcare Network Accreditation Commission (EHNAC) - Section 5: Security

Subject: **5. Security**	
Subsection: **5.2 Administrative Safeguards**	Effective Date:
Author:	Original Date:
Review by:	Revision Date:
Approval by:	Document Reference:

I. Purpose
GeHC will ensure proper security for PHI.

II. Policy
The GeHC will conduct quarterly internal and annual 3rd party compliance audits and assessments of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI held by the Guam HIE.

III. Procedure:
The GeHC will conduct quarterly internal and annual 3rd party compliance audits and assessments of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI held by the Guam HIE in accordance with Administrative Safeguards.

The GeHC will apply appropriate sanctions against Board members, employees, contractors, volunteers, trainees, and others whose conduct is under the direct control of the GeHC (whether or not they are paid by the GeHC) with access to PHI who are not in compliance with the security policies and procedures of the GeHC. Sanctions may include (but is not limited to) suspension of user access.

The GeHC and their contractors will maintain a listing of all hardware and software used to store transmit or maintain e- PHI, including all Primary Domain Controllers (PDCs) and servers. Documentation must be provided showing which software resides on which hardware. This documentation will be available for inspection at each PO and through the Privacy Officer.

IV. Definitions:

V. References/Related Policies:
45 C.F.R. § 164.308(a)(1)(ii)(A) and (C): http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=932f8fd8eaf00b36bb3a3e932cc69545&n=45y1.0.1.3.79&r=PART&ty=HTML#45:1.0.1.3.79.3.27.4
The Electronic Healthcare Network Accreditation Commission (EHNAC) - Section 5: Security

Subject: **5. Security**	
Subsection: **5.3 Privacy Officer Responsibilities**	Effective Date:
Author:	Original Date:
Review by:	Revision Date:
Approval by:	Document Reference:

I. Purpose
GeHC will ensure proper security for PHI.

II. Policy
The GeHC will train and employ a Privacy Officer.

III. Procedure:
The GeHC has identified a Privacy Officer, and their backup designee, who is responsible for the development, implementation and enforcement of the policies and procedures required by the Privacy and Security Rules. These responsibilities will be documented, including a description of their specific responsibilities, and communicated internally. This person is also responsible for receiving complaints and providing individuals with information on the GeHC's privacy practices as they relate to the Guam HIE. The GeHC Privacy Officer is also expected to work with the GeHC Board and POs in the event that a privacy issue arises.

The GeHC Privacy Officer will regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports and maintain/report discrepancies. This regular review, in addition to compliance audits, is designed to detect patterns of inappropriate access, use and disclosure. The GeHC Privacy and Security Officer has the power to recommend changes to privacy and security policies and procedures

IV. Definitions:

V. References/Related Policies:
45 C.F.R. § 164.308(a)(2): http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=932f8fd8eaf00b36bb3a3e932cc69545&n=45y1.0.1.3.79&r=PART&ty=HTML#45:1.0.1.3.79.3.27.
The Electronic Healthcare Network Accreditation Commission (EHNAC) - Section 5: Security

Subject: **5. Security**	
Subsection: **5. Physical Safeguards**	Effective Date:
Author:	Original Date:
Review by:	Revision Date:
Approval by:	Document Reference:

I. Purpose
GeHC will ensure proper security for PHI.

II. Policy
The GeHC shall limit physical access to its electronic information systems and the facility or facilities in which they are housed, while also providing that all properly authorized persons have adequate access.

III. Procedure:
The GeHC will evaluate the adequacy of controls on physical access to facilities and equipment handling of PHI as part of its information security risk assessment of each PO. As part of its risk management plan, a PO should document and have available for inspection, the facility access control and equipment handling logs. If a PO does not control the building they occupy or shares space with other organizations, it nonetheless remains responsible for considering facility security. It can incorporate security measures into contracts with the party responsible for the building and document them in their own plan.

The GeHC will safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

A PO must evaluate the need for, and adequacy of controls on physical access to facilities and equipment handling PHI as part of risk management plan and Facility Security Plan. POs should document its approach to controlling physical access to facilities and equipment handling protected health information. Unauthorized physical access to the facility may be limited via door locks, electronic access control systems, security officer (for larger facilities), and video monitoring. Additionally, facilities will have major doors re-keyed, door combinations changed, and/or key cards destroyed after the termination of employees or contractors with prior access to facilities that stored e-PHI.

IV. Definitions:

V. References/Related Policies:
45 C.F.R. § 164.310(a)(1), (2): http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=932f8fd8eaf00b36bb3a3e932cc69545&n=45y1.0.1.3.79&r=PART&ty=HTML#45:1.0.1.3.79.3.27.5

The Electronic Healthcare Network Accreditation Commission (EHNAC) - Section 5: Security

Subject: **5. Security**	
Subsection: **5. Movement and Destruction of media**	Effective Date:
Author:	Original Date:
Review by:	Revision Date:
Approval by:	Document Reference: Facility/Hardware Log

I. Purpose
GeHC will ensure proper security for PHI.

II. Policy
The GeHC will follow general best practices in the final disposition of e- PHI and/or the hardware or electronic media on which it is stored.

III. Procedure:
GeHC will utilize the 'Facility/Hardware Log' governing the receipt and removal of hardware and electronic media that contains e-PHI into and out of a facility, and the movement of these items within the facility.

Before transferring computers containing any software, GeHC will ensure it is properly licensed to transfer the item, that it was not obtained illegally or in violation of license terms, and that the software was never copied illegally or in violation of license terms. The transfer must conform to terms of the software license.

Internal software license inventory records should be updated to reflect any transfer or deletion of software. Electronic media that contains e-PHI must be rendered unusable or inaccessible. Degaussing uses a magnetic field to erase the data. Destroying the media makes the data inaccessible. If circumstances warrant the destruction of the electronic media prior to disposal, destruction methods may include disintegrating, pulverizing, melting, incinerating, or shredding the media. Covered entities may contract with business associates to perform these services for them.

The GeHC will follow best practices in the industry for removal of e-PHI from electronic media before the media are made available for re-use. Certain steps are taken to remove the e-PHI stored on the computers or other media before its disposal or reuse, or if the media itself is destroyed before its disposal. The HIPAA Security Rule requires that covered entities address the final disposition of e-PHI and/or the hardware or electronic media on which it is stored, as well as to implement procedures for removal of e-PHI from electronic media before the media are made available for reuse.

Depending on the circumstances, appropriate methods for removing e-PHI from electronic media prior to reuse or disposal may be by clearing (using software or hardware products to overwrite media with non-sensitive data) or purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains) the information from the electronic media. Internal re-use may

include redeployment of PCs or sharing disks. All e-PHI previously stored on the media must be removed prior to reuse to prevent unauthorized access to the information.

The GeHC will dispose of all technology hardware, software and paper records in accordance with federal, state, and local laws, including, but not limited to regulating waste and respecting copyright and licensed software. In addition, GeHC will ensure that sensitive information is protected and follow all HIPPA specific policies and procedures. In the event a department possesses technology hardware or software that is no longer required due to:

1. Excess of useful life
2. Lack of continued need
3. Unable to upgrade required hardware or software
4. Damage
5. Excessive maintenance cost
6. Received a new computer

All such equipment will be returned to the GeHC central office for evaluation. Workforce employees will be trained to avoid printing any document with PHI.   Unnecessary paper product that contains PHI will be shredded as soon as possible and cannot remain in an employee's work area.

The GeHC and/or PO will create a retrievable exact copy of e-PHI before movement of equipment where PHI is stored. The PO must include in their risk management plan the procedure to create and maintain data backups and retrievable exact copies of e-PHI. The appropriate backup mechanism (e.g., magnetic tapes, paper, or other medium), back-up location (e.g., offsite, in an air conditioned compartment or other conditions), and duration of copy (e.g., six months or following state/territory or federal guidelines for patient records) will be determined. A PO may create a hard drive back-up before moving to prevent loss of E-PHI. The GeHC also reserves the right to limit where information can be stored and require that all information to be saved on the network.

IV. Definitions:

V. References/Related Policies:
45 C.F.R. § 164.310(d)(1), (2)(i): http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=932f8fd8eaf00b36bb3a3e932cc69545&n=45y1.0.1.3.79&r=PART&ty=HTML#45:1.0.1.3.79.3.27.5
The Electronic Healthcare Network Accreditation Commission (EHNAC) - Section 5: Security

Subject: **5. Security**	
Subsection: **5.6 Technical Safeguards**	Effective Date:
Author:	Original Date:
Review by:	Revision Date:
Approval by:	Document Reference:

I. Purpose
GeHC will ensure proper security for PHI.

II. Policy
GeHC will ensure electronic information systems that maintain e-PHI to allow access only to those persons or software programs that have been granted access rights.

III. Procedure:

Access
The GeHC restricts the role-based access to the HIE based on the authorized user's current employment responsibilities. Workforce employees will have their access level noted in the HIE usage file and be reviewed regularly by their supervisor and/or the Privacy Officer. Changes in access levels will be made quickly and documented in the employee's file. The access is first authorized then later access requests are approved or disapproved based on the previously defined authorizations.

The GeHC will establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process in accordance with The user will receive the level of access that ensures only the minimum necessary access to provide care. Additionally, the POs and BAs will attest to the appropriateness of the roles assigned and the corresponding access level for that user. Evidence of this documentation will be available for inspection at each PO and reviews coordinated through the Privacy Officer.

The access controls process will check that the user has been authorized to use that resource/module. Users must be authorized to access information through the HIE that is consistent with the job functions as determined by the PO. POs are required to quarterly audit user accounts and compare the information accessed to the care provided by the authorized user. GeHC will implement periodic security updates, reminders and refresher programs for the members of the Workforce, including management.

Passwords
The GeHC shall have specific procedures for creating, changing, and safeguarding passwords and/or other login procedures.

Each PO's Workforce shall receive password management training covering industry recommended guidelines. This includes but is not limited to: devising secure passwords, storing/remembering

passwords, and avoidance of sharing passwords. System administrators will require passwords to be changed every ninety (90) days.

Workforce members are prohibited from sharing computer login information, including password(s) with others or leave their written password(s) in a place that could be accessible by others. If a user has reason to believe others have learned their password(s), they will report the problem to their supervisor and will take appropriate action to have the password(s) reset. Furthermore, it is prohibited that workforce will not attempt to use the logins and passwords of others, nor allow their logins and passwords to be used by others. Under HIPAA law, employees must change their passwords regularly to assure PHI data is safeguarded.

System Shutdown

System administrators will ensure that after three failed login attempts; authorized users will be locked out of the system until they obtain clearance from the administrator to resume normal activities. Unusual usage by an authorized user will generate an alert to the system Administrator/Security Officer.

Additionally, authorized users will be logged out of the system after ten minutes of inactivity. Terminated employees will have their accounts disabled immediately and applicable security entry changes or removed. Users shall be required and trained to logoff the system when their workstation is unattended.

Usernames

The GeHC will assign a unique name and/or number for identifying and tracking all systems' user identity. All authorized users will receive a unique user name that is connected to all authentication attempts. A unique identifier allows GeHC or a PO to track specific user activity when that user is logged into an information system. Users can be held accountable for functions performed on information systems with e-PHI when logged into these systems. User identification is a way to identify a specific user of an information system, typically by name/number. At a minimum, the employee name or some variation of the name can be used. However, a better system is a set of random numbers and characters. This may be harder for an authorized user to remember but more likely to keep an unauthorized user from gaining inappropriate access.

The GeHC will record and examine activity in information systems that contain or use e-PHI. The HIE will establish warnings and automatic e-mail alerts to the Security Officer when erratic usage or other anomalies by an authorized user is detected.

IV. Definitions:

V. References/Related Policies

45 C.F.R. § 164.312(a)(1), (2), (b): http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=932f8fd8eaf00b36bb3a3e932cc69545&n=45y1.0.1.3.79&r=PART&ty=HTML#45:1.0.1.3.79.3.27.6

45 C.F.R. §164.308(a)(4)(ii)(B)-(C), and (a)(5)(ii)(D): http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=932f8fd8eaf00b36bb3a3e932cc69545&n=45y1.0.1.3.79&r=PART&ty=HTML#45:1.0.1.3.79.3.27.4

The Electronic Healthcare Network Accreditation Commission (EHNAC) - Section 5: Security

Subject: **5. Security**	
Subsection: **5. Emergencies or Disasters**	Effective Date:
Author:	Original Date:
Review by:	Revision Date:
Approval by:	Document Reference: Emergency Treatment Disclosure

I. Purpose
GeHC will ensure proper security for PHI.

II. Policy
The GeHC shall have appropriate procedures for accessing necessary e- PHI during an emergency or disaster.

III. Procedure:

Emergency Access
The GeHC enables providers to access PHI in emergency situations by overriding patient consent policies. Immediate consent in emergency situations may not be readily available, so written consent will be obtained after the emergency service is provided as 'Emergency Treatment Disclosure'.

Additionally, the GeHC will include a determination if POs are appropriately using their emergency access privileges in the audit process. Emergency Treatment Disclosure access is terminated upon completion of the emergency treatment and evidence of such is available for later inspection through compliance audits.

POs shall develop and implement alternate means of obtaining PHI during such emergencies until normal controls are restored. POs shall identify appropriate approaches to this problem during their information security risk assessment and document them in their contingency plans. These plans will be available for review and inspection.

Disaster Access
Fire, vandalism, natural disaster, or system failure sometimes damage safeguards to the confidentiality, integrity and availability of protected health information. This implementation specification requires POs to develop and implement alternate means of PHI during such emergencies until normal controls are restored. GeHC shall maintain secure facility access in support of restoration of lost data under the disaster recovery and emergency mode operations in their risk management plan. The GeHC will establish, document, and implement emergency mode operations plans to enable continued protection of the e-PHI.

Testing of Disaster Recovery
There are documented procedures for periodic testing, assessment, review and revision of disaster recovery and emergency mode operation plans. Testing and all appropriate revisions coordinated through GeHC should occur no less than annually.

Random testing will serve as training for those with a role in the risk management plan and as assurance that the plan is appropriate. Failures in the testing process provide a means for corrective action and plan improvement.

System Back-up

Each PO must create and maintain data backups. The "data backup" portion of a risk management plan should ensure that information will not be lost in the event of a major system loss or catastrophic event. The rule requires each health information system risk management plan to include procedures for performing "exact copies" of individually identifiable patient information (backups) for retrieval when necessary.

Each PO must determine what information requires back up, the appropriate backup mechanism (e.g., magnetic tapes, paper, or other medium), how to maintain the backups (e.g., offsite, in an air conditioned compartment or other conditions), and duration of maintenance (e.g., six months or following state/territory or federal guidelines for patient records) as part of its risk analysis including its application and data criticality analyses. Data backup is required at regular intervals and a full system backup will be completed monthly. The risk management plan should document the backup policies and procedures, including provisions for periodically reviewing and updating them.

Risk Management

Each PO shall be required to have a risk management plan for recovering from a disaster. Their risk analyses including application and data criticality analysis will determine the order, interval of time, and the methods chosen for recovery. POs will identify appropriate approaches to this problem during their information security risk assessment and document them in their risk management plans. These plans will be available for review and inspection.

Each PO must plan to protect PHI during an emergency. POs will identify appropriate approaches to this problem during their on-site assessments and document them in a risk management plan. This may include additional security at entrances or escorts for authorized users to the facility for data restoration purposes.

IV. Definitions:

V. References/Related Policies
45 C.F.R. § 164.312(a)(2)(ii): http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=932f8fd8eaf00b36bb3a3e932cc69545&n=45y1.0.1.3.79&r=PART&ty=HTML#45:1.0.1.3.79.3.27.6
45 C.F.R. § 164.310(a)(2)(i): http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=932f8fd8eaf00b36bb3a3e932cc69545&n=45y1.0.1.3.79&r=PART&ty=HTML#45:1.0.1.3.79.3.27.5
45 C.F.R. § 164.308(a)(7)(ii)(C): http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=932f8fd8eaf00b36bb3a3e932cc69545&n=45y1.0.1.3.79&r=PART&ty=HTML#45:1.0.1.3.79.3.27.4

The Electronic Healthcare Network Accreditation Commission (EHNAC) - Section 5: Security

Subject: **5. Security**	
Subsection: **5. Business Associate Contracts**	Effective Date:
Author:	Original Date:
Review by:	Revision Date:
Approval by:	Document Reference:

I. Purpose
GeHC will ensure proper security for PHI.

II. Policy
The GeHC requires BAs to implement administrative, physical, and technical policies and procedures that protect the confidentiality, integrity, and availability of the e-PHI it creates, receives, maintains, or transmits on behalf of the GeHC.

III. Procedure:
The GeHC will require BAs to implement administrative, physical, and technical policies and procedures that are reasonable, appropriate, and required by federal and state law to protect the confidentiality, integrity, and availability of the e-PHI it creates, receives, maintains, or transmits on behalf of the GeHC in accordance with These policies and procedures will be reviewed for approval and then again every five years by the BA and the GeHC Board.

The GeHC will have BA contracts in place that obtain satisfactory assurances that the BA will uphold applicable federal and state/territory regulations. BAs will be required to use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and will help the covered entity comply with some of the duties under the Privacy Rule. Covered entities may disclose PHI to an entity in its role as a BA only to help the covered entity carry out its health care functions – not for the BA's independent use or purposes, except as needed for the proper management and administration of the BA.

The GeHC will require BAs to ensure that any agent, including a subcontractor, to whom it provides such information, agrees to implement reasonable and appropriate policies and procedures.

GeHC will require BAs to report any security incident it becomes aware of – directly to the GeHC within 24 hours. The BA must notify the GeHC Privacy Officer immediately upon discovery of the incident. Any unauthorized acquisition, access, use or disclosure of PHI that compromises the security or privacy of the PHI would be considered a HIPAA security incident or breach. Examples include: a lost laptop that is not encrypted, lost or stolen paper applications and misdirected mail. This requirement does not replace existing breach notification state/territory laws. BAs must comply with both federal requirements and any applicable state/territory law requirements.

The GeHC will terminate a BA's contract in the event they determine that the BA has violated a material term of the contract. The GeHC will ensure BAs are contractually required to comply with all applicable federal and state/territory regulations including HITECH privacy and security requirements.

All BAs notify the GeHC in the event any PHI is improperly used or disclosed, including for the purpose of the breach notification rule. GeHC must promptly notify affected individuals of a breach, as well as the HHS Secretary and the media in cases where a breach affects more than 500 individuals. Breaches

affecting fewer than 500 individuals will be reported to the HHS Secretary on an annual basis. The regulations also require BAs to notify the covered entity of breaches at or by the BA. The GeHC shall have BAAs in place with every organization that it contracts with for the purpose of exchanging or routinely accessing e- PHI.

IV. Definitions:

V. References/Related Policies:
45 CFR § 164.502(e)(2).
HITECH §13404(b),
45 CFR §§ 164.314(a)(2)(i)(B) (C).(D)
HITECH §13408,
The Electronic Healthcare Network Accreditation Commission (EHNAC) - Section 5: Security

Subject: **6. Consent**	
Subsection: **6.1 Patient Consents**	Effective Date:
Author:	Original Date:
Review by:	Revision Date:
Approval by:	Document Reference:

I. Purpose

The GeHC will ensure that required patient consents are consistently obtained throughout the HIE.

II. Policy

The GeHC shall describe its approach to patient consent to participate in the HIE (i.e., opt-in, opt-out, or no consent required, and change of consent) in a related policy statement as well as information provided to consumers.

III. Procedure:

Consumers will have some control over the exchange of their PHI through the Guam HIE based on the model that is finalized. 'Opt-in' requires the consumer's authorization via written consent. 'Opt-out' requires that notice is provided to the consumer that their PHI is exchanged and puts the responsibility on the consumer to formally request exclusion from the HIE.

POs are required to annually attest that they have conducted compliance audits confirming alignment with written authorizations for access. GeHC may conduct annual and random audits with individual POs to ensure compliance with federal privacy and security legislation.

Education on consumer's rights to opt-out is handled within each PO by registration and admission staff as well as nurses and others within emergency departments. GeHC will provide training and readiness assessments of staff to inform consumers of the exchange and their right to opt out. All registration and admissions staff interfacing with patients will be trained accordingly. Evidence of this training will be available for inspection in the training file.

GeHC provides appropriate procedures for patient-initiated change of consent at any time provided that the change does not preclude any PHI previously accessed by HIE trading partners.

GeHC shall specify the patient consent required to query their PHI. Consumers are informed at the points of registration or admission within a PO. Copies of a related brochure (created by the GeHC and POs) are available at these locations for patients. On the brochure are several frequently asked questions about the HIE and the direct messaging service currently implemented. There is also a description of the opt-out right and consequences.

IV. Definitions:

V. References/Related Policies

The Electronic Healthcare Network Accreditation Commission (EHNAC) - Section 6: Consent

Subject: **6. Consent**	
Subsection: **6.2 Public Health Reporting**	Effective Date:
Author:	Original Date:
Review by:	Revision Date:
Approval by:	Document Reference:

I. Purpose

The GeHC will ensure that required patient consents are consistently obtained throughout the HIE.

II. Policy

GeHC maintains policies and procedures for the release of information to a government agency as mandated by law or as permitted by HIE policy.

III. Procedure:

Public health reporting may include birth, death, disease, child abuse, domestic violence, exposure to communicable disease, and/or health oversight activities. If a consumer has 'opted out' of HIE disclosure, PHI will not be released except as required by law or for public heath reporting requirements as noted. The consumer's PHI in this situation is captured outside of the exchange.

IV. Definitions:

V. References/Related Policies

The Electronic Healthcare Network Accreditation Commission (EHNAC) - Section 6: Consent

Subject: **6. Consent**	
Subsection: **6.3 Emergency Treatment**	Effective Date:
Author:	Original Date:
Review by:	Revision Date:
Approval by:	Document Reference:

I. Purpose

The GeHC will ensure that required patient consents are consistently obtained throughout the HIE.

II. Policy

The GeHC enables providers to access PHI in emergency situations by overriding patient consent policies.

III. Procedure:

Immediate consent in emergency situations may not be readily available, so written consent will be obtained after the emergency service is provided as 'Emergency Treatment Disclosure'. Additionally, the GeHC will include a determination if POs are appropriately using their emergency access privileges in the audit process.

The GeHC ensures that 'Emergency Treatment Disclosure' access is terminated upon completion of the emergency treatment and evidence of such is available for later inspection through compliance audits.

IV. Definitions:

V. References/Related Policies

The Electronic Healthcare Network Accreditation Commission (EHNAC) - Section 6: Consent

Subject: **6. Consent**	
Subsection: **6.4 Minors**	Effective Date:
Author:	Original Date:
Review by:	Revision Date:
Approval by:	Document Reference:

I. Purpose
The GeHC will ensure that required patient consents are consistently obtained throughout the HIE.

II. Policy
The GeHC maintains specific policies regarding PHI for minors.

III. Procedure:
The GeHC will respond appropriately to minors' requests to keep certain categories of their PHI confidential and to exercise the rights granted to patients by the HIPAA in accordance with federal laws and regulations.

HIPAA provides individuals with certain rights related to their PHI, including the right to request their PHI be kept confidential. Although minors do not generally have the authority to exercise rights on their own behalf, state law and HIPAA provides minors with the authority to exercise control over certain categories of their own PHI.

IV. Definitions:

V. References/Related Policies
The Electronic Healthcare Network Accreditation Commission (EHNAC) - Section 6: Consent

Subject: **7. Authorization**	
Subsection: **7.1 User Categories**	Effective Date:
Author:	Original Date:
Review by:	Revision Date:
Approval by:	Document Reference:

I. Purpose
GeHC shall maintain a user authorization process (includes all trading partners/users in the HIE).

II. Policy
Access control will be appropriately planned, controlled and executed throughout GeHC and it's POs.

III. Procedure:
The access control process is divided into two phases: 1) policy definition phase where access is authorized, and 2) policy enforcement phase where access requests are approved or disapproved based on the previously defined authorizations.

Access controls rely on authentication to verify the user identify. The access controls process will validate that the user has been authorized to use that resource/module. Users must be authorized to access information through the HIE that is consistent with the job functions as determined by the PO. User authorization is critical to establishing user accountability and managing risk.

The GeHC restricts the role-based access to the HIE based on the authorized user's current employment responsibilities. Workforce employees will have their access level noted in the HIE usage file and be reviewed regularly by their supervisor and/or the Privacy Officer. Changes in access levels will be within one week and documented in the employee's file. The access is first authorized then later access requests are approved or disapproved based on the previously defined authorizations.

IV. Definitions:

V. References/Related Policies
The Electronic Healthcare Network Accreditation Commission (EHNAC) - Section 7: Authorization

Subject: **8. Authentication**	
Subsection: **8.1 Proof of Identity**	Effective Date:
Author:	Original Date:
Review by:	Revision Date:
Approval by:	Document Reference:

I. Purpose
The GeHC will ensure correct authentication for users.

II. Policy
The GeHC maintains requires proof of identity for authorized users.

III. Procedure:
To provide maximum protection of PHI, the GeHC will require the HIE, and/or trading partner entities, to verify proof of identity for their authorized users upon application for access to the HIE. Additionally, authentication will take place at each user attempt to access the information.

Authentication steps will include (but not be limited to): user name and password, device recognition, and security question(s).

This 2-factor authentication is required for users of all modules (Direct secure messaging, RLS query, Security Manager and Consent Manager).   Authorized personnel at each facility are responsible for identifying and managing the staff accessing the HIE within their organization Including both Direct secure messages and query-based transactions.

To ensure HIPAA compliance, all communication through the Guam HIE will be fully encrypted, using a Public Key Infrastructure (PKI) security model, to ensure that the identity of the client and server can be cryptographically verified. Additionally, all transactions will be logged to ensure full audit capabilities.

IV. Definitions:

V. References/Related Policies
The Electronic Healthcare Network Accreditation Commission (EHNAC) - Section 8: Authentication

Subject: **8. Authentication**	
Subsection: **8.2 Encryption**	Effective Date:
Author:	Original Date:
Review by:	Revision Date:
Approval by:	Document Reference:

I. Purpose

The GeHC will ensure correct authentication for users.

II. Policy

The GeHC will encrypt user authentication data.

III. Procedure:

All authorized users will receive a unique user name that is connected to all authentication attempts. As part of the regular audits of POs, the GeHC will investigate and verify authentication logs. These logs will be maintained for a length of time to meet or exceed state/territory and federal requirements.

The GeHC will ensure the following:
1. Authentication data is secure as it is entered;
2. Authentication data is administered properly;
3. Authentication actions are recorded corresponding to unique users; and
4. Security of active and non-active user IDs and passwords.

IV. Definitions:

V. References/Related Policies

The Electronic Healthcare Network Accreditation Commission (EHNAC) - Section 8: Authentication

Subject: **9. Access**	
Subsection: **9.1 Authorized Purposes**	Effective Date:
Author:	Original Date:
Review by:	Revision Date:
Approval by:	Document Reference:

I. Purpose
The GeHC will regulate access based on user role and purpose.

II. Policy
The GeHC shall permit authorized users to access PHI only for the purposes consistent with the patient's consent status or as permitted by HIPAA, and state/territory and federal law. This includes the use of patient registries.

III. Procedure:
All users will be assigned one or more roles/privileges for accessing information. Only those with appropriate authorization may access PHI. User functions are identified as:

1. Patient Query and Discovery (used by most users)
2. Audit Log Query and Reporting (used by authorized privacy and security officers)
3. Consent Management (used by authorized personnel to manage opt out requests received from POs).

Authorized Users will be logged out of the system within 10 minutes of inactivity. After three failed login attempts, authorized users will be locked out of the system until reinstated by the System Administrator. Unusual usage by an authorized user will generate an alert to the Privacy Officer.

The administrative policies and procedures established in Information Access Management under the Administrative Safeguards section of the Security Rule identify and determine the access rights and privileges of authorized users. A covered entity's IT systems must enforce those administrative policies. This standard includes two related mandatory implementation specifications: unique user identification and emergency access procedure, and three addressable implementation specifications: automatic logoff, encryption and decryption, and mechanism to restrict access.

GeHC shall ensure that that RLS includes reasonable safeguards to minimize unauthorized incidental disclosures of PHI during the process of identifying a patient and locating the record. The search algorithms will have a positive match threshold set high to reduce false positives. Localized patient IDs will be used when available. Additionally, 'wildcard matching' will be prohibited.

IV. Definitions:

V. References/Related Policies
The Electronic Healthcare Network Accreditation Commission (EHNAC) - Section 9: Access

Subject: **9. Access**	
Subsection: **9.2 Personnel Training and Termination**	Effective Date:
Author:	Original Date:
Review by:	Revision Date:
Approval by:	Document Reference:

I. Purpose
The GeHC will regulate access based on user role and purpose.

II. Policy
The GeHC shall have minimum training requirements for educating authorized users about the policies and procedures for accessing PHI through the HIE. Additionally, GeHC will follow a specific procedure to commence the access termination process or suspension process for authorized users.

III. Procedure:
These training requirements must be fulfilled as of the date of hire, annually and as needed (as deemed by Privacy Officer). The evidence of training completion will be available for inspection in the employees' training files.

GeHC will follow access termination process or suspension process for authorized users in situations of misuse or employment status changes. This may lead to the imposition of additional sanctions or criminal charges for violators. Upon entry to the HIE, POs and other HIE participants will be informed of incidents that could lead to termination of access (e.g. inappropriate disclosure or access of PHI). In the event of a violation, the GeHC will review the violation and immediately notify the user and/or PO of the actions. The GeHC will sanction the user accordingly but will consider reinstatement of access and will also review user appeals after an investigation of the incident.

The GeHC shall implement a termination procedure for immediately withdrawing access to electronic PHI when the employment of a Workforce member ends, the Workforce member's duties no longer justify the need to access PHI, or as required by determinations made as specified in the previous criterion. Terminated employees will have their accounts removed and discontinued immediately.

The GeHC will ensure that all members of the Workforce have access only to e-PHI necessary to perform their specific work assignment, and will prevent access for those Workforce members who do not have a need to access e- PHI. Workforce members, BAs, and contractors with authorized access will be identified by title and/or job function.

The 2-factor authentication is required for users of all modules (RLS query, Security Manager and Consent Manager). Authorized personnel at each facility are responsible for identifying and managing the staff accessing the HIE within their organization including Direct secure messages and query-based transactions.   Additionally, POs have internal policies requiring all staff, contractors, etc. to adhere to federal and state/territory privacy laws.

The GeHC shall document procedures to determine that the access of a Workforce member, vendor, contractor and their employees to e- PHI is appropriate and is limited to only that which is necessary to the performance of work duties in accordance. Workforce members, BAs, and contractors with authorized access will be identified by title and/or job function.

IV. Definitions:

V. References/Related Policies
The Electronic Healthcare Network Accreditation Commission (EHNAC) - Section 9: Access

Subject: **10. Audit**	
Subsection: **10.1 Disclosure Logs**	Effective Date:
Author:	Original Date:
Review by:	Revision Date:
Approval by:	Document Reference:

I. Purpose
The GeHC will ensure track PHI disclosure for auditing purposes.

II. Policy
The GeHC will maintain disclosure logs for the systems by which authorized users access PHI. Upon request, patients can have access to information about disclosures of their health information.

III. Procedure:
The GeHC will maintain disclosure logs by the HIE and/or POs for the systems by which authorized users access PHI, including:

1. The identity of the patient whose PHI was accessed;
2. The identity of the authorized user accessing the PHI;
3. The identity of the trading partner with which such authorized user is affiliated;
4. The type of PHI or record accessed (e.g., pharmacy data, laboratory data, etc.);
5. The date and time of access; and
6. The source of the PHI (i.e., the identity of the trading partner from whose records the accessed PHI was derived).

The GeHC will control secure disclosure logs from alteration regardless of access privilege and will log any attempted alterations. The GeHC shall require that disclosure logs be maintained for at least six (6) years from the date when the information was accessed.

The GeHC will provide patients, upon request, with access to information from the HIE and/or POs about disclosures of their health information. The disclosure report will draw from the full disclosure log and include the name of the individual that that received the PHI, the affiliated organization, the date of disclosure, and the specific information disclosed. This report will be available to the consumer without cost (by request)within 30 days of the request. Notification will be sent to the particular PO if requests are received from a patient.

The GeHC requires that patients be informed of the availability of such information on any patient portals maintained by the HIE. Additionally, the process for requesting the report will be communicated and readily available.

IV. Definitions:

V. References/Related Policies
The Electronic Healthcare Network Accreditation Commission (EHNAC) - Section 10: Audit

Definition of Terms

Addressable:
Addressable refers to implementation specifications contained within certain HIPAA Regulations, which GeHC not required to implement. GeHC must perform an assessment to determine whether the addressable implementation specification is a reasonable and appropriate safeguard for implementation in its efforts to protect unauthorized use, disclosure, and access of PHI or ePHI. If it is not reasonable and appropriate, GeHC must document the reasons supporting this conclusion.

Administrative Safeguards:
Administrative Safeguards are actions, policies and procedures to manage the selection, development, implementation, and maintenance of security measures to protect ePHI and to manage the conduct of Users in relation to the protection of ePHI.

Breach:
The unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.

Business Associate:
A Business Associate is a person or entity who, on behalf of a Covered Entity, performs, or assists in the performance of, a function or activity involving the use or disclosure of individually identifiable health information, including, but not limited to, facilitation of the exchange of health information; claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; or practice management.

Contingency Event:
An unplanned event, such as an emergency or disaster, which may require the activation of the Contingency Plan, Data Back-Up Plan, Disaster Recovery Plan, or Emergency Operations Plan.

Covered Entity:
A Covered Entity is (i) a health plan, (ii) a health care clearinghouse, or (iii) a health care provider who transmits any health information in any form, including in electronic form. For purposes of this HIPAA Privacy and Security Policy and Procedures Manual, Covered Entity means a Direct Secure Messaging Subscriber who utilizes Direct Secure Messaging, including health care providers, medical practices, and laboratories.

Direct Secure Messaging:
A service provided by Direct Subscribers that allows the Subscriber to send and receive secure messages utilizing the Direct Project specifications and an internet-based service provided by DC-HIE, through a contracted HISP.

Electronic Protected Health Information or ePHI:
Electronic PHI means PHI, which is either transmitted by electronic media or maintained in electronic media.

HIPAA Regulations:
HIPAA Regulations means the Health Insurance Portability and Accountability Act of 1996 and the rules and regulations and related updates, and the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. §§ 17921-17954) and the rules or regulations and related updates.

Physical Safeguards:
Physical Safeguards are physical measures, policies, and procedures to protect the Network and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Protected Health Information or PHI:
PHI, also referred to as protected health information, generally refers to demographic information, medical history, test and laboratory results, insurance information and other data that is collected by a health care professional to identify an individual and determine appropriate care.

Required:
Required refers to implementation specifications contained within certain HIPAA regulations with which GeHC must comply.

Security Incident:
The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations of Direct Secure Messaging.

Technical Safeguards:
Technical Safeguards means the technology and the policy and procedures that GeHC has in place to protect ePHI and control access to it.

User:
A person or entity with authorized access to Direct Secure Messaging. Users include workforce members, Direct Secure Messaging Subscribers, employees and agents of GeHC who are authorized to use Direct Secure Messaging and Vendors.

Vendor:
Vendor means a vendor, consultant, contractor or other non-GeHC third party who may have access to the Network for any reason or purpose (other than those who may have incidental access) or who may have access to any facilities housing the information technology assets that support the Network or related infrastructure.

Workforce Member:
All persons who are under the control of GeHC, including, but not limited to, employees, independent contractors, loaned personnel, interns, and temporary personnel who have access to the Network or any PHI derived from the Network.

Workstation: Workstation means an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

APPENDIX C: Required Reporting Definitions and Sources

PIN Priority	Numerator	Denominator	Source
1. **% of pharmacies participating in e-prescribing**	Number of pharmacies that sent or received any electronic new prescription, refill request, or refill response messages in December of the former year via Surescripts network	Total number of licensed pharmacies operating in the state (per NCPDP)	Surescripts/NCPDP data ***ONC will provide data to Grantees***
2. **% of labs sending electronic lab results to providers in a structured format[1]**	Number of hospital and independent clinical laboratories that send electronic lab results to ambulatory care providers in a structured format	Total number of hospital and independent clinical laboratories that respond to census	*Numerator: data collected through Grantee's lab census (a sample instrument will be provided following the release of this PIN)* *Denominator: Census should target all labs in "hospital" and "independent" lab categories, including LabCorp and Quest, in CLIA OSCAR database (*http://wwwn.cdc.gov/clia/oscar.aspx*)* ***Grantee assesses. ONC will provide a sample instrument.***
3. **% of labs sending electronic lab results to providers using LOINC**	Number of hospital and independent clinical laboratories that send electronic lab results to ambulatory care providers using LOINC	Total number of hospital and independent clinical laboratories that respond to survey	*Numerator: data collected through Grantee's lab census* *Denominator: Census should target all labs in "hospital" and "independent" lab categories, including LabCorp and Quest, in CLIA OSCAR database (*http://wwwn.cdc.gov/clia/oscar.aspx*)* ***Grantee assesses. ONC will provide a sample instrument.***

---

[1] **Structured format:** Documentation of discrete data using controlled vocabulary, creating fixed fields within a record or file, or another method that provides clear structure to information (is not completely free text).

PIN Priority	Numerator	Denominator	Source
4. **% of hospitals sharing electronic care summaries with (a) unaffiliated hospitals and (b) unaffiliated providers**	Number of non-federal acute care hospitals sharing electronic clinical care summaries with the following entities as reported in the AHA HIT Supplement survey: a. Hospitals outside their system b. Ambulatory care providers outside their system	Total number of non-federal acute care hospitals responding to AHA HIT supplement survey	AHA HIT supplement survey *ONC will provide data to Grantees annually. Grantees may expect an annual release in December or January.*
5. **% of ambulatory providers electronically sharing care summaries with other providers**	Number of ambulatory care, office-based physicians who share electronic clinical summaries or summary of care records with other providers	Total number of ambulatory care, office-based physicians who responded to the survey	National Ambulatory Medical Care Survey (NAMCS) Electronic Medical Records (EMR) Supplement (also known as National Electronic Health Records Survey) **ONC will provide data to Grantees annually. Grantees may expect an annual release in December or January.**
6. **Public Health agencies receiving ELR data produced by EHRs or other electronic sources in HL7 2.5.1 format with LOINC and SNOMED.**	1= Yes 0= No (or %) **ANSWER** NONE		Grantee assesses

PIN Priority	Numerator	Denominator	Source
7. **Immunization registries receiving electronic immunization data produced by EHRs in HL7 2.3.1 or 2.5.1 formats using CVX codes.**	1= Yes 0= No (or %) **ANSWER** NONE		Grantee assesses
8. **Public Health agencies receiving electronic syndromic surveillance data from hospitals produced by EHRs in HL7 2.3.1 or 2.5.1 formats (using CDC reference guide)**	1= Yes 0= No (or %) **ANSWER** Not at this time but plan on using the HIE to receive this data		Grantee assesses
9. **Public Health agencies receiving electronic syndromic surveillance ambulatory data produced by EHRs in HL7 2.3.1 or 2.5.1 formats.**	1= Yes 0= No (or %) **ANSWER** Not at this time but plan on using the HIE to receive this data		

APPENDIX D - Tracking Program Progress for HIE Adoption: Target Goals and Achievements

See Appendix C for measure definitions and sources

Program Priority	Report in first SOP update			Report January, 2013			Report January, 2014	
	Status as of December, 2011	Target for December, 2012		Status as of December, 2012	Target for December, 2013		Status as of December, 2013	Target for end of grant period
1. % of pharmacies participating in e-prescribing	0%	25%		0%	25%		TBD	75%
2. % of labs sending electronic lab results to providers in a structured format[2]	0%	25%		0%	25%		TBD	50%
3. % of labs sending electronic lab results to providers using LOINC	0%	25%		0%	25%		TBD	50%
4. % of hospitals sharing electronic care summaries with unaffiliated hospitals and providers	0%	100%		0%	100%		TBD	100%

---

[2] **Structured format:** Documentation of discrete data using controlled vocabulary, creating fixed fields within a record or file, or another method that provides clear structure to information (is not completely free text).